AI Generated Deepfake Financial Scams: A Missing Liability Regime For Consumer Protection Frameworks

Alison Lui* and Andrea Miglionico**

The authors declare no conflicts of interest regarding this manuscript.

Competing interests: The author(s) declare none

Abstract

Generative artificial intelligence (GenAI) outputs, such as deepfakes, can be useful for creating realistic simulations in education, news reporting and arts. However, the emergence of malicious deepfake scams has raised concerns about the quality and reliability of the information provided to social media users. This article argues that a liability regime for deepfakes is currently missing from consumer protection frameworks. It posits that regulatory interventions do not explicitly target GenAI software developers and online social media platforms, which should be required to implement appropriate risk management safeguards to prevent unlawful activities. We contend that a shared liability regime for deepfakes among the multiple actors involved could offer adequate protection for victims of online financial fraud and would effectively target the deepfake supply chain. This shared liability regime is complemented by the UK Financial Conduct Authority's Consumer Duty rule, which acts as a preventive monitoring and enforcement mechanism to avoid foreseeable harm to customers in AI applications.

1. Introduction

The rapid proliferation of GenAI has resulted in sophisticated technologies that are readily available and easy for scammers to create convincing-looking content.[1] Deepfake scams are complex threats that target, deceive and manipulate customers across industries through for example, synthetic videos and imagery; and scammers use online social media platforms available to them and constantly adapt to evade enforcement.[2] The scams are using deepfakes of celebrities in videos to trusted professionals, which is causing a growing concern for the

* Liverpool John Moores University, Faculty of Law; A.Lui@ljmu.ac.uk.

** University of Reading, School of Law; a.miglionico@reading.ac.uk.

The authors are grateful to the reviewers for their constructive and insightful comments on earlier drafts.

[1] GenAI is a technology based on the use of machine learning and multi-layered neural networks which perform through a large dataset. Ardi Janjeva, Alexander Harris, Sarah Mercer, Alexander Kasprzyk and Anna Gausen, 'The Rapid Rise of Generative AI: Assessing risks to safety and security' (December 2023), Research Report, Alan Turing Institute, Centre for Emerging Technology and Security, https://cetas.turing.ac.uk/sites/default/files/2023-12/cetas_research_report_-_the_rapid_rise_of_generative_ai_-_2023.pdf.

[2] Jon Bateman, *Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios* (July 2020), Cyber Policy Initiative Working Paper Series "Cybersecurity and the Financial System", p.20-21.

finance sector.[3] There is consensus that deepfakes can produce outputs that are not explicitly programmed and are occasionally inaccurate with the intent to cause distress to the recipient.[4] A 2024 survey by Regula reveals that globally, half of all businesses have experienced fraud involving audio and video deepfakes.[5] Additionally, 66% of leaders believe deepfakes pose a serious threat to their business; on average, businesses across industries have lost nearly $450,000 to deepfakes.[6] This faces multifaceted challenges for public authorities, particularly around legal and ethical implications such as consent, misleading content and cybersecurity.[7]

The consequences for individual customers may be irreparable if deepfakes distort relevant information in providing financial advice or assistance crucial for the decision-making process.[8] Deepfakes are working like a charm for scammers because social media users simply do not know what GenAI is capable of when it comes to making convincing impersonation videos.[9] Users watch deepfake videos and believe they are real, because many do not have the information or knowledge to question it. As reported, 'ordinary people use a product or service in the real world may diverge wildly from the designers' intentions in the lab'.[10] Deepfakes are increasingly being used on video calls to impersonate senior staff at corporate organisations, persuading other staff members to process payments which turn out to be fraudulent.[11] As the technology progresses, deepfakes have the potential to make romance scams even more convincing, and could potentially be used to manipulate images of friends and family relatives

[3] AI-driven scams are becoming increasingly sophisticated, thereby intensifying the risks faced by consumers. Scam warnings are issued to alert individuals to potential fraud involving offers of loans that require an upfront fee, often made by individuals posing as representatives of legitimate financial firms. Offering financial products on behalf of unauthorised intermediaries is fraudulent, and victims of such scams are advised to contact their bank immediately and report the incident to action fraud. See Joshua Franklin, Stephen Gandel and Akila Quinio, 'Who should foot the bill for cyber scams?' *Financial Times* (London, 11 December 2024), https://www.ft.com/content/577dff0d-b7a0-4bc3-a1b1-3ca828e5ba18.

[4] Lauren E. Willis, 'Deception by Design' (2020) 34(1) *Harvard Journal of Law & Technology* 115; Bobby Chesney and Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107(6) *California Law Review* 1753.

[5] See https://regulaforensics.com/news/deepfake-fraud-doubles-down/.

[6] Henry Patishman, 'The Impact of Deepfake Fraud: Risks, Solutions, and Global Trends' (15 November 2024), https://regulaforensics.com/blog/impact-of-deepfakes-on-idv-regula-survey/.

[7] Adrienne de Ruiter, 'The Distinct Wrong of Deepfakes' (2021) 34(4) *Philosophy & Technology* 1311.

[8] Michal Lavi and Hadar Yoana Jabotinsky, 'Seeing is Believing? Deepfakes in Financial Markets' (2026) 44(1) *Cardozo Arts & Entertainment Law Journal* 55.

[9] Claer Barrett and Maisie Grice, 'The rise of deepfake scams — and how not to fall for one' *Financial Times* (London, 2 May 2025), https://www.ft.com/content/fcbdc88f-bbfd-4338-915a-9ef7970b2123.

[10] John Thornhill, 'We are the new gremlins in the AI machine' *Financial Times* (London, 26 June 2025), https://www.ft.com/content/aaa57d4b-fee6-4109-87ac-9222d706fe07.

[11] Liz Lumley, 'Deepfake fraud directed at banks on the rise' *The Banker* (12 June 2025), https://www.thebanker.com/content/14c72a58-3723-5a0f-b3f7-fb95108f7fda.

making requests for money.[12] This practice creates a social problem and could threaten resilience assets such as networks, human relationships, individual education, and media trust.[13]

Scammers are relentless and continuously evolve their tactics to try and escape detection. This pushes firms to develop new ways to make it harder for fraudsters to deceive others including using facial recognition technology.[14] There is a general assumption that business-to-consumer uses of digital platforms[15] can be sufficiently regulated through existing contracts, tort (e.g., fault-based liability based on negligence) and consumer protection laws.[16] Contractual mechanisms for limiting the scope of responsibility for professional advice are considered in terms of consumer protection policy.[17] Extant debates focus on holding deepfake content creators accountable.[18] There are, however, challenges with this. Copyright and data protection laws seem inadequate to impose liability on creators of deepfakes due to questions of anonymity and authorship, as well as difficulties in bringing an action for copyright infringement of any underlying copyright works.[19] The question at stake is how copyright

[12] Synthetic technologies incorporate sophisticated algorithmic systems, such as generative adversarial networks (GANs), which operate through a generator that produces synthetic media and a discriminator that evaluates and refines the data to enhance the realism of the generated content. See Baoping Liu, Bo Liu, Tianqing Zhu and Ming Ding, 'A Review of Deepfake and Its Detection: From Generative Adversarial Networks to Diffusion Models' (2025) *International Journal of Intelligent Systems*, https://doi.org/10.1155/int/9987535.

[13] Ebba Lundberg and Peter Mozelius, 'The potential effects of deepfakes on news media and entertainment' (2025) 40(4) *AI & Society* 2159.

[14] Chris Newlands, 'Goldman's deepfake problem: Can the real David Kostin please stand up?' *The Banker* (9 May 2025), https://www.thebanker.com/content/dd99dbb8-ea39-4993-8d6b-6e5c8ba0ea0e.

[15] The terms 'digital platforms', 'online platforms' and 'online social media platforms' are used interchangeably. Legislation such as the UK Online Safety Act uses the term 'digital platform', whilst the EU Digital Services Act uses 'online platform'. Our focus is on online social media platforms and our shared liability regime applies to online social media platforms.

[16] Kathryn E. Spier and Rory Van Loo, 'Foundations for Platform Liability' (2025) 100(3) *Notre Dame Law Review* 1137; Gökçe Kurtulan-Güner, 'Platform Liability: Quo Vadis?' (2020) 9(3) *Journal of European Consumer and Market Law* 275; James Grimmelmann and Pengfei Zhang, 'An Economic Model of Online Intermediary Liability' (2023) 38(3) *Berkeley Technology Law Journal* 1011; Teresa Rodriguez de las Heras Ballell, 'The Role of Digital Platforms' Liability in Regulating Global Value Chains: The EU's Approach' (2024) 59(2) *Texas International Law Journal* 15.

[17] Mateja Durovic and Chris Willett, 'A Legal Framework for Using Smart Contracts in Consumer Contracts: Machines as Servants, Not Masters' (2023) 86(6) *Modern Law Review* 1390.

[18] Jane C. Ginsburg and Graeme W. Austin, 'Regulating Deepfakes at Home and Abroad' (2025) 48(3) *Columbia Journal of Law & the Arts* 297; Felipe Romero Moreno, 'Generative AI and deepfakes: a human rights approach to tackling harmful content' (2024) 38(3) *International Review of Law, Computers & Technology* 297; Rebecca A. Delfino, 'Deepfakes on Trial: A Call to Expand the Trial Judge's Gatekeeping Role to Protect Legal Proceedings from Technological Fakery' (2023) 74(2) *Hastings Law Journal* 293; Yi Yan, 'Deep Dive into Deepfakes - Safeguarding Our Digital Identity' (2023) 48(2) *Brooklyn Journal of International Law* 767.

[19] It is worth noting that AI-generated content is generally not protected by copyright in most jurisdictions unless substantial human input is involved, and even in such cases there is no guarantee that copyright protection will be granted. This raises the question of who owns the rights to AI-generated material, which largely depends on the presence of an identifiable human author. On this point see Hannah Yee-Fen Lim, 'Generative AI Output for Business Organizations: Legal Perspectives from Copyright Law' in Wai Fong Boh, Chee Hua (Neumann) Chew

applies to the use of protected works in training generative AI models, particularly at the data collection and model training stages, which impose legislative frameworks to focus on strengthening licensing, transparency and enforcement regulatory measures.[20] Investigations are very costly and time-consuming.[21] Criminal penalties would not be suitable to deter deepfake content creators, as they require proof beyond a reasonable doubt of the intention to deceive consumers.[22] Similarly, social media platforms release their own policies for removing or banning deepfakes, which use 'intent' as their barometer for deciding whether to remove a deepfake. However, defining 'intent' is highly subjective, since it is based on the assessment of individual actors.

At the EU level, the General Data Protection Regulation introduced an articulated set of penalties on companies that fail to protect the data of citizens.[23] The European Artificial Intelligence Act (EU AI Act)[24] and Digital Services Act (DSA) 2022[25] show limitations to accommodate liability for AI-generated harms.[26] The EU legislation has not provided a clear definition of malicious deepfakes, making meaningless any responsibility of the deepfake

and Thara Ravindran (eds), *Data Strategy and AI Value Creation* (Singapore: World Scientific Publishing 2025) 197.

[20] House of Lords, Communications and Digital Committee, 'AI, copyright and the creative industries' (6 March 2026) 4th Report of Session 2024–26, HL Paper 267, https://publications.parliament.uk/pa/ld5901/ldselect/ldcomm/267/267.pdf.

[21] Dennis Crouch, 'Using Intellectual Property to Regulate Artificial Intelligence' (2024) 89(3) *Missouri Law Review* 781; John T. Kivus, 'Generative AI and Copyright Law: A Misalignment That Could Lead to the Privatization of Copyright Enforcement' (2024) 25(3) *North Carolina Journal of Law & Technology* 447. See also Barry Scannell, 'Who owns the copyright for AI work?' *Financial Times* (London, 24 August 2025), https://www.ft.com/content/74b1841f-bf57-4934-a06a-3611d61e4319.

[22] Jacquelyn Sherman, 'A Feast of Fraud: How International Hesitations to Regulate Deepfakes Are Creating a Buffet for Financial Criminals' (2025) 56(1-2) *George Washington International Law Review* 91.

[23] Regulation (EU) 2016/679. See also Yi Yan, 'Deep Dive into Deepfakes - Safeguarding Our Digital Identity' (2023) 48(2) *Brooklyn Journal of International Law* 767.

[24] Regulation (EU) 2024/1689.

[25] Regulation (EU) 2022/2065.

[26] Guido Noto La Diega and Leonardo C.T. Bezerra, 'Can there be responsible AI without AI liability? Incentivizing generative AI safety through ex-post tort liability under the EU AI liability directive' (2024) 32(1) *International Journal of Law and Information Technology*, https://doi.org/10.1093/ijlit/eaae021; Martina J. Block, 'A Critical Evaluation of Deepfake Regulation through the AI Act in the European Union' (2024) 13(4) *Journal of European Consumer and Market Law* 184.

supply chain.[27] Under the UK's Online Safety Act (OSA) 2023,[28] technology companies must set performance targets to remove illegal material quickly when they become aware of it and test algorithms to make illegal content harder to disseminate.[29] The OSA 2023 introduced offences prohibiting the creation, sharing and threatening to share intimate images, including deepfakes. In the context of financial scams, the Act imposes a duty on digital platforms to 'use proportionate measures relating to the design or operation of the service'[30] and 'operate the service using proportionate systems and processes designed'[31] so that users cannot view fraudulent content and that platforms remove such content as soon as possible. Nevertheless, the OSA 2023 does not impose direct liability on digital platforms towards victims of fraudulent scams.

A shared liability regime for GenAI scams would target the deepfake AI supply chain, which involves multiple actors such as the creator of the video, the developer of the software (the company provider) used to fabricate the altered or distorted image, the online platforms that intermediate the dissemination of the video, and digital users for uploading, viewing and sharing the content. Supply chains are complex networks of interconnected third parties, cloud services, and IT systems that face risks of cyberattacks in AI models and systems exposed to misuse of datasets.[32] The creator of the video or perpetrator usually makes non-consensual deepfake materials that are claimed to be lawful and legitimate, while they are the result of 'an unauthorised exploitation and reengineering of other people's images and thus, their personal

[27] Despite the fact that EU legislation does not expressly classify deepfakes as high-risk AI systems, Article 82(3) of the Act requires Member States to disclose information about the supply chain of automated applications. Directive (EU) 2022/2555 on Network and Information Systems (NIS2) provides that Member States must adopt a national cybersecurity strategy, including policies on supply chain security, vulnerability management, and cybersecurity education and awareness. The NIS2 Directive applies to a wide range of sectors, including providers of public electronic communications, digital services such as social media platforms, waste and wastewater management, critical product manufacturing, postal and courier services, public administration at both central and regional levels, and the space sector. See EU Commission, 'NIS2 Directive: securing network and information systems', https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[28] See https://www.legislation.gov.uk/ukpga/2023/50/contents.

[29] Beatriz Kira, 'When non-consensual intimate deepfakes go viral: The insufficiency of the UK Online Safety Act' (2024) 54 *Computer Law & Security Review*, https://doi.org/10.1016/j.clsr.2024.106024.

[30] OSA 2023, s 27(2).

[31] OSA 2023, s 27(3).

[32] AI attackers exploit opportunities within supply chain ecosystems, where a single centralised software service supports multiple organisations, thereby exposing weaknesses in the detection of cyber vulnerabilities. See the findings of the World Economic Forum, 'Global Cybersecurity Outlook 2024' (January 2024) Insight Report, p.33, https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf. See also Chuck Brooks, 'The Growing Cybersecurity Risks To The Supply Chain In The AI Era' *Forbes* (22 May 2026), https://www.forbes.com/sites/chuckbrooks/2026/05/22/the-growing-cybersecurity-risks-to-the-supply-chain-in-the-ai-era/.

data'.[33] The company providers are responsible for writing the code, integrating third-party components, and ensuring that the development of software is immune from vulnerabilities and threats. Developers of software hold the delicate task of implementing coding practices that ensure security and integrity of the decision-making process.[34] Several episodes of manipulated machine learning models in supply chains resulted in undesirable outputs because a threat scammer accessed a supply chain and jeopardised the algorithm.[35] AI models are more exposed to manipulation as is the case with the technique of feeding adversarial data to the training data set of the model in a way that gives biases or errors without triggering security mechanisms.[36] Poisoning AI models with malicious code within software components to control the results is a common method in deepfake scams where large databases are exploited to alter key automated procedures.[37]

The liability regime would prescribe AI software developers and online social media platforms to apply for a licence before the implementation of software applications. Regulatory sandboxes offer a suitable tool for testing AI-generated systems in a legally controlled environment while providing accuracy on AI recommendations and screening potential

[33] European Parliament, 'Tackling deepfakes in European policy' (July 2021) European Parliamentary Research Service, Panel for the Future of Science and Technology, PE 690.039, p.50, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf.

[34] The management and maintenance of software applications and infrastructure (e.g. security, compliance, and performance monitoring) form part of supply chain operations. The process of software development and delivery—from planning and design through development, testing, deployment, and operations—complements the supply chain lifecycle. For an overview see Aamiruddin Syed, *Supply Chain Software Security. AI, IoT, and Application Security* (Apress Berkeley, CA, 2024) p.28-29.

[35] The case of the Iberian Peninsula blackout, which disrupted the Portuguese National Health Service in April 2025, demonstrated failures in power supply, digital systems, telecommunications, and inter-institutional coordination. This incident exposed the health sector's vulnerabilities to cyberattacks and energy disruptions, highlighting the need for regulatory improvements and decentralised energy solutions. See Francisco Goiana-da-Silva et al., 'When the lights went out: impacts of the April 2025 Iberian blackout on the Portuguese National Health Service sovereignty - a reflection on national defence, health sovereignty, risk, and infrastructural dependency' (July 2025) 13 *Frontiers in Public Health*, doi: 10.3389/fpubh.2025.1630933.
An instructive example of a manipulated AI model is the Trading Algorithm Catastrophe of July 2025, which involved a significant incident in which a quantitative hedge fund's flagship AI trading algorithm began exhibiting erratic behaviour during periods of high market volatility. The algorithm had been compromised during pre-training, with embedded triggers designed to activate under specific market conditions. This case highlighted the challenges of regulating modern algorithmic strategies in interconnected derivatives markets. See Winston Wei Dou, Itay Goldstein and Yan Ji, 'AI-Powered Trading, Algorithmic Collusion, and Price Efficiency' (July 2025) NBER Working Paper 34054, https://www.nber.org/papers/w34054.

[36] Oladoyin Akinsuli, 'AI-Powered Supply Chain Attacks: A Growing Cybersecurity Threat' (2024) 8(3) *Iconic Research and Engineering Journals* p.700, https://www.irejournals.com/formatedpaper/1706490.pdf.

[37] Aditya K. Sood and Sherali Zeadally, 'Malicious AI Models Undermine Software Supply-Chain Security' (June 2025) 68(6) *Communications of the ACM*, p. 66, https://doi.org/10.1145/3704724. The authors pointed on the cases of SolarWinds and Kaseya ransomware attacks as poisoned software within supply chain structures.

malicious deepfakes in financial products.[38] Singapore Courts have adopted a comprehensive binding Guide on GenAI use to verify the accuracy and appropriateness of all AI-generated outputs.[39] The Guide attributes full responsibility for the content of AI tools to court users; however, the question is: who should be liable for the losses of deepfake scams when the supply chain for the scam is highly complicated?

The UK Financial Conduct Authority (FCA)'s consumer duty rule, which established regulatory standards against firms' unfair practices, can provide a solution to the exploitation of financial scams in the use of GenAI tools.[40] The duty mandates financial firms to evaluate their products, services and processes in view to protect customers in business relationships and remedy foreseeable harms.[41] Its purpose is to set higher expectations for the standard of care that firms afford to customers while, in parallel, making firms responsible for addressing fraudulent practices that impede consumers from achieving reliable outcomes. However, the duty rule is primarily a financial regulation principle and does not explicitly apply across all sectors. It might not be suitable to mitigate detrimental generated outputs of deepfake scams.

We argue that the shared liability regime for deepfakes would combine with the consumer duty rule as a regulatory conduct of business for firms to assess the suitability of their financial advice services and monitor the results of AI-generated content that customers receive. This could require online social media platforms to share liability for losses with financial firms which, in turn, leads to the development of a preventive enforcement mechanism for the consumer protection framework. We contend that a shared liability regime in malicious financial deepfakes between content creators, software developers and online social media platforms would be effective as a form of deterrence to hold these actors liable for fraudulent scams.

The originality of the proposed shared liability framework lies in the analysis of various actions and activities among multiple parties which serves to understand potential scenarios where the

[38] Jennifer Calver, Peter Church, Jonathan Ford and Kim Rust, 'AI in financial services - the legal and regulatory landscape' in Jelena Madir (ed), *FinTech: Law and Regulation* (3rd edn., Cheltenham: Edward Elgar 2024) ch.16.
[39] See 'Guide on the Use of Generative Artificial Intelligence Tools by Court Users' Registrar's Circular No. 9 2024,
https://www.judiciary.gov.sg/docs/default-source/circulars/2024/registrar's_circular_no_9_2024_state_courts.pdf?sfvrsn=d038ec05_1.
[40] FCA, 'A new Consumer Duty. Feedback to CP21/36 and final rules' (July 2022), Policy Statement PS22/9, p.40, https://www.fca.org.uk/publication/policy/ps22-9.pdf.
[41] Sandra Booysen, 'Protecting Consumers from Payment Fraud: An International Perspective' paper presented at the 2nd International Conference the Responsible Consumer in the Digital Age: 'Evolving Perspectives on Consumer Protection, Sustainability, and AI – the Nordics and Beyond', Copenhagen, 28 April 2025.

apportionment of responsibilities involves each actor in the AI supply chain. Although the idea of shared liability has been shaped in various contexts according to the main doctrinal views, the distinctiveness of this model advances existing debates in the AI parlour while providing critical reflections on the need for further regulatory intervention and redress policy options. However, the limitations of the proposed framework point to the difficulty of identifying the portion of liability of each actor's action in every stage of the supply chain; the existing regulatory regimes do not allocate the loss when an AI system causes harm, and the degree of accountability for one's behaviour is not equivalent to the attribution of responsibility which mostly depends on context and the AI application used. Furthermore, the victim of the harm bears the onerous burden of proving which decision-making process in the supply chain led to the specific outcome, a difficult proof especially in a system where the procedures are not fully reliable or detectable.

The article proceeds as follows. We begin with an introduction of GenAI techniques, illustrating how they elaborate content and produce outputs that are not explicitly programmed. Section 2 examines the regulatory framework of deepfakes in the UK, which is the focus of the article. However, we also discuss the regulatory frameworks of deepfakes in the EU and Singapore as a comparison. In the UK, we place particular attention to the OSA 2023 and its main effects on regulated services. The EU comparative analysis is useful because the main piece of legislation, the DSA 2022, adopts a systems-based approach in contrast to the content based approach in the OSA 2023. Comparison with Singapore is instructive because it has a lower threshold for scams and malicious cyber activities than the UK. The Singaporean government only needs to suspect that there is online harm to issue a direction, while for other activities, reasonable suspicion is required. This contrasts with the 'reasonable grounds to infer' that the content amounts to an offence in section 192(5) of the OSA 2023 for all offences including scams and cyber activities. Further, the Singaporean legislation providers faster remedies to scam victims than in the UK.

Section 3 depicts the liability contours of deepfake financial scams, analysing the challenges to identifying the responsible party for GenAI fraud. This section addresses the liability attribution to deepfake content creators and the interaction with online social media platforms: it investigates the applicable regulatory standard to hold liable the fraudsters and to ensure

effective consumer protection through compensation schemes for scam losses.[42] Platform responsibility in investment scams is also considered along with potential challenges in imposing liability on scam victims. This leads to the elaboration of a framework which establishes obligations on the various actors in the deepfake supply chain. Section 4 advances a policy proposal for a shared liability regime to prevent multiple actors from disseminating malicious deepfakes in financial investments. We identify potential scenarios which allocate responsibility to content creators, software developers, online social media platforms as the main actors involved in online fraudulent activities. In this context, we define content creators as the authors and creators of deepfake scams advertised as posts on regulated online social media platforms such as Facebook or Instagram, which host the deepfake content. Software developers are the individuals and businesses which created the deepfake software enabling deepfake scams. Section 5 concludes and outlines final remarks.

2. The Regulatory Landscape for Deepfakes in the UK

The OSA 2023 represents the most significant attempt to protect consumers by regulating harmful online content including deepfakes. It regulates search services that allow users to post content online or to interact with each other. Regulated services must have 'links' with the UK, either because they have a 'significant number' of users, or they view the UK as a target market, or they can be accessed from the UK and there 'are reasonable grounds to believe that there is a material risk of significant harm to individuals' from their content.[43] While it creates new duties for internet service providers,[44] it has several limitations regarding deepfakes. First, the Act focuses primarily on protection from illegal content and content harmful to children. Illegal content is defined in Schedules 5-7, and the priority offences (which include fraud and financial services offences) are broadly defined in Schedule 7. However, there are far more non-

[42] In Australia, the Scams Prevention Framework Act 2025 introduced preventive measures against scams in key sectors such as banking, telecommunications and digital platforms to ensure compensation schemes for victims of fraud. The legislation requires service providers to take various actions to combat scams relating to their services. See https://www.legislation.gov.au/C2025A00015/asmade/text.
[43] OSA 2023, s 4(2), 4(5) and 4(6).
[44] The OSA 2023 imposes extensive duties on internet service providers in relation to online communication, transparency reporting, content moderation and verification of user's ages. Department of Science, Information and Technology, 'Guidance Online Safety Act: Explainer' (Department of Science, Information and Technology, 24 April 2025), https://www.gov.uk/government/publications/online-safety-act-protection-of-children-codes-of-practice-explanatory-memorandum.

financially related offences under Schedule 7 such as pornography and sexual abuse compared to fraud.[45]

Further, different types of harms call for different legal treatment. With intentional misuse of generative AI tools such as deepfake voice cloning or synthetic identity creation used to defraud, harm arises from malicious user behaviour. Here, the actor(s) with fraudulent intent to deceive and harm others should be liable, while platforms and service providers face obligations under the OSA to implement proportionate systems to detect, mitigate, and remove such illegal content. Regulators focus on content moderation and criminal enforcement here.

Meanwhile, unintended harms from faulty AI outputs, such as incorrect information generated through hallucinations, involve questions of product reliability, safety, and duty of care.[46] The relevant legal areas are negligence and product liability. Product developers need to ensure model accuracy, explainability and user safeguards. The regulatory concerns here are algorithmic accountability and transparency. Thus, while both intended and unintended harms involve AI-generated content, the legal treatment is different. Intended harms involve monitoring misuse by users and governing malfunction, whilst unintended harms concern rectifying design defects in AI outputs.

Second, critics such as Nash and Felton argue that legislation should focus more on regulating digital platforms as systems rather than just hosts of content.[47] The OSA currently adopts a content-based regulatory approach, where it imposes duties on regulated services regarding the content uploaded on platforms. The OSA tackles the aspect of removing illegal content and content and activity harmful to children (section 1(2) of the OSA). However, this neither directly tackle human vulnerabilities nor hold the responsible actor(s) liable to a criminal standard. Criminal liability would fall under existing criminal offences such as fraud by false representation (section 2 of the Fraud Act 2006) in the UK.

Taking the example of a celebrity's image being used in a fraudulent deepfake advertisement for a cryptocurrency investment scheme uploaded on an online social media platform,[48] the

[45] ibid.
[46] Alex Casey, 'Generative AI's Duty to Deal Dilemma' (2026) 36(2) *Albany Law Journal of Science & Technology* 1.
[47] Victoria Nash and Lisa Felton, 'Treating the symptoms or the disease? Analysing the UK Online Safety Act's approach to digital regulation' (2024) 16(4) *Policy and Internet* 818.
[48] A customer from NatWest bank in the UK lost £150,000 in a deepfake video scam where Martin Lewis, a money savings expert, was impersonated. Tali Ramsey, 'Scam alert: deepfake videos are on the rise' (17 July 2024) *Which?*, https://www.which.co.uk/news/article/scam-alert-deepfake-videos-are-on-the-rise-aIlx30B9keja.

OSA 2023 criminalises fraudulent advertising, which can be either a Category 1 or Category 2A regulated service, depending on the threshold conditions regarding the type of service and number of users.[49] Under a Category 1 service, internet service providers must comply with more duties than those in Category 2A or 2B. For instance, companies must put in place proportionate systems and processes to prevent (or minimise in the case of search engines in Category 1A) the publication and hosting of fraudulent advertising on their service. Companies must also remove it when they are made aware of it. Non-compliance can lead to criminal liability for named senior managers.

Despite the promise to regulate scam advertisements, the OSA 2023 is unable to cope with the 'cat and mouse' game of removing harmful online content. TikTok removed 85.8 million pieces of content in quartile 4 of 2021[50] while Instagram removed 43.8 million pieces of content in the same period.[51] Even with content moderators working at full speed, it is difficult to keep pace with the vast amount of content uploaded every day. Further, although deepfakes can be malicious and harmful, the most damage they can cause is when they are operating in conjunction with other technological tools such as cryptocurrency wallets, QR codes and manipulation of platform engagement metrics.[52] We illustrate this with the example of Elon Musk's image being used in a deepfake cryptocurrency scam. On 18 June 2024, scammers illegally obtained $50,000 in cryptocurrency in just two hours with a deepfake video of Musk soliciting investments via a YouTube livestream. Viewers who invested were first deceived through the deepfake video of Musk. The video was streamed on YouTube channels with a high number of subscribers. Scammers then rebranded them to impersonate the official Tesla YouTube channel before launching a livestream.

The scammers directed the investors offline through a QR code to invest. Moving investors offline and onto their mobile phones has the benefit of less content moderation and scam detection.[53] Therefore, effective regulation requires thorough processes by user-to-user

[49] Category 1 service means "a regulated user-to-user service for the time being included in the part of the register established under subsection (2)(a)" of the OSA.
[50] TikTok, TikTok Community Guidelines Enforcement, Q3 2021.
[51] Ofcom, 'Just one in six young people flag harmful content online' (16 March 2023), https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/one-in-six-young-people-flag-harmful-content-online?language=en.
[52] Shaurya Malwa, 'Weaponized Trading Bots Drain $1M From Crypto Users via AI-Generated YouTube Scam' (7 August 2025), https://www.coindesk.com/tech/2025/08/07/weaponized-trading-bots-drain-usd1m-from-crypto-users-via-ai-generated-youtube-scam.
[53] Max Rizzuto, 'Crypto-scam hosts pop-up livestream featuring a deepfaked Elon Musk' (DFR Lab, 25 September 2024), https://dfrlab.org/2024/09/25/musk-deepfake-crypto-scam/.

services to identifying the risks when deepfakes are working alongside generative AI, QR codes, search engines.[54] The highly convincing deepfake video is only one element that contributed to the fraud. Anonymity and opacity from moving cryptocurrency in several wallets, manipulating subscriber numbers and diverting investors offline through a QR code all contributed to the sophisticated fraud. This case illustrates that deepfake investment scams often operate in a landscape of other technological tools and platforms, which makes it difficult to attribute the precise attribution of liability to individual actors involved.

The *modus operandi* of deepfake enabled financial scams is varied though. Deepfake scammers can directly target senior company leaders such as the widely reported case of deepfake financial scam of the Hong Kong office of a UK company called Arup. In the case of Arup, the company lost $25 million to a deepfake conference video.[55] This case did not involve the use of social media platforms, so the deepfake supply chain is shorter but nonetheless cross-border in nature. Therefore, there are varied methods of committing financial deepfake scams, which ultimately exploit human, not organisational system vulnerabilities.[56]

Farrand posits that the OSA is too narrow since it focuses on individual 'psychological or physical' harms to specific users and not systemic harms that affect the wider society.[57] Deepfake financial scams do not fall into this definition because they are non-linear, networked, algorithmically amplified and cross multiple platforms rather than via individual content.[58] The OSA does not tackle the systemic conditions in the fraud ecosystem. By contrast, the EU DSA 2022 requires very large online platforms to assess and reduce systemic risks arising from algorithmic design, amplification dynamics and manipulation techniques (Recitals 69; Art. 34 DSA). As a result, the OSA's content-based approach struggles to address the infrastructural and behavioural drivers of deepfake financial scams, whereas the DSA's systemic-risk

[54] ibid.
[55] Leng Cheng and Ho-Him Chan, 'Arup lost $25mn in Hong Kong deepfake video conference scam' *Financial Times* (London, 17 May 2024), https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea.
[56] Raúl Carrillo, 'Platform Money' (2024) 41(3) *Yale Journal on Regulation* 894, 940.
[57] Benjamin Farrand, 'How Do We Understand Online Harms? The Impact of Conceptual Divides on Regulatory Divergence between the Online Safety Act and Digital Services Act' (2024) 16 *Journal of Media Law* 240, https://doi.org/10.1080/17577632.2024.2357463.
[58] Petter Törnberg, 'Echo chambers and viral misinformation: Modeling fake news as complex contagion' (2018) 13(9) *PLoS ONE*, e0203958, https://doi.org/10.1371/journal.pone.0203958. See also Ioannis Agrafiotis, Jason R C Nurse, Michael Goldsmith, Sadie Creese and David Upton, 'A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate' (2018) 4(1) *Journal of Cybersecurity* 1, https://doi.org/10.1093/cybsec/tyy006.

framework is expressly designed to regulate the platform-level mechanisms that make such harms scale.

2.1 The Legal Framework in the EU

Article 50(4) of the EU AI Act[59] sets out disclosure requirements for "deployers of an AI system that generates or manipulates image, audio or video content constituting a deep fake".[60] Labelling AI generated or manipulated content improves transparency and enables users to know, especially when several studies support that customers find it difficult to establish whether AI generated media is real or not.[61] Similar to the EU AI Act, the US AI Labelling Act 2023 requires developers of generative AI systems to disclose "clear and conspicuous information indicating the content includes the use of AI". Wittenberg et al. show that labelling can reduce an individual's chance of relying on and engaging with misleading AI generated images.[62]

With the public possessing varying levels of knowledge and familiarity with generative AI, designing effective labels with the appropriate content is key to preventing deepfake fraud.[63] However, empirical studies demonstrated that authorship labels can be effective to enhance transparency, although they are unlikely to affect the persuasiveness of the labelled content, requiring alternative techniques to address risks posed by AI-generated information.[64] Wittenberg et al. opine that labels of whether content has been generated or manipulated by AI are process based and are not as effective as labelling content as 'manipulated' or 'false', which

[59] Regulation (EU) 2024/1689.
[60] We use the term 'deployers' to indicate professional users of AI systems. Under Article 3 of the EU AI Act, 'AI system' means "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".
[61] Kimberly T. Mai, Sergi D. Bray, Toby Davies and Lewis D. Griffin, 'Warning: Humans Cannot Reliably Detect Speech Deepfakes' (2023) 18(8) *PLoS ONE*, https://doi.org/10.1371/journal.pone.0285333. See also Hany Farid, 'Creating, Using, Misusing, and Detecting Deep Fakes' (2022) 1(4) *Journal of Online Trust and Safety*, https://www.tsjournal.org/index.php/jots/article/view/56.
[62] Chloe Wittenberg, Ziv Epstein, Adam J. Berinsky and David G. Rand, 'Labeling AI-generated media online' (2025) 4(6) *PNAS Nexus*, https://doi.org/10.1093/pnasnexus/pgaf170.
[63] Sacha Altay and Fabrizio Gilardi, 'People are skeptical of headlines labeled as AI-generated, even if true or human-made, because they assume full AI automation' (2024) 3 *PNAS Nexus*, https://doi.org/10.1093/pnasnexus/pgae403.
[64] Isabel O. Gallegos, Chen Shani, Weiyan Shi, Federico Bianchi, Izzy Gainsburg, Dan Jurafsky and Robb Willer, 'Labeling Messages as AI-Generated Does Not Reduce Their Persuasive Effects' (July 2025), Policy Brief HAI Policy & Society, Stanford University, https://hai.stanford.edu/assets/files/hai-policy-brief-labeling-ai-generated-content.pdf.

is impact based. The latter is more effective in changing people's behaviour.[65] Ternovski et al.'s experiments reveal that general labels warning the public about videos led to the public distrusting *all* videos are fake, even if they were real.[66] Further, the participants in the experiments did not show any improvement in identifying manipulated videos. Therefore, research to date shows that targeted labelling appears to be more effective than general labelling.

Articles 34 and 35(1)(k) of the EU DSA 2022[67] also mandate very large online platforms to conduct thorough risk analyses, curb the dissemination of illegal content and label deepfakes and false information. Although this systems-based framework has its advantages, there are a few weaknesses. The "notice and action" mechanism in Article 16 of the Act allows individuals or entities to ask online platforms to remove illegal content. However, Article 16(2) sets out conditions for activating the 'notice and action' mechanism, one of which requires the individual or the entity to provide "a sufficiently substantiated explanation of the reasons" why they think the content is illegal. This seems rather difficult for the public to determine what is "illegal content" when the definition in Article 3(h) of the EU DSA 2022 is broad and vague. Whilst the content of child abuse is clearly illegal, the public needs to provide reasons why this is illegal. This means searching for suitable legal authorities. For non-lawyers, this can be an onerous task. Indeed, De Steel et al. report that many stakeholders, such as non-governmental organisations are of the view that the users "are not necessarily capable of accurately identifying illegal content online".[68] The users can only make assumptions that the content is likely to be illegal.

Content moderators compare the content on platforms against databases storing illegal content such as the Image Watch List by the Internet Watch Foundation.[69] This process, called hash-matching, is made more difficult because generative AI can reproduce edited versions of the

[65] Wittenberg et al. (n 62).
[66] John Ternovski, Joshua Kalla, and Peter Aronow, 'The Negative Consequences of Informing Voters about Deepfakes: Evidence from Two Survey Experiments' (2022) 1(2) *Journal of Online Trust and Safety*, https://tsjournal.org/index.php/jots/article/view/28/15.
[67] Regulation (EU) 2022/2065.
[68] Alexandre De Steele, Elise Defreyne, Hervé Jacquemin, Michèle Ledger and Alejandra Michel, 'Online Platforms' Moderation of Illegal Content Online: Law, Practices and Options for Reform' (Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, June 2020).
[69] See https://www.iwf.org.uk/.

same illegal content very quickly, bypassing databases which hold illegal content.[70] Further, auto-detection software such as watermarking and labelling methods used by online platforms present weaknesses.[71] In particular, they are not very effective with shorter texts, content translated from other languages, or factual replies and they implicitly treat synthetic media as false and deceptive.[72] Whilst there are databases for illegal child abuse (IWF Watch List and Interpol),[73] there do not appear to be similar ones for fraud. Even for established databases for illegal content, Stockwell et al. suggest that it is important that these repositories use standardised metrics, such as harmonised labelling and classification methods.[74] Standardisation of repositories would be helpful given the global nature of the internet and its related problems.

2.2 The Regulatory Approach in Singapore

Singapore adopted a piece of legislation specifically targeting deepfakes in political elections. The Elections (Integrity of Online Advertising) Bill of 2024[75] bans the publication, boosting, sharing and reposting of deepfake content depicting election candidates. This adds to the protection given in the Online Safety (Miscellaneous Amendments) Act 2022[76] and Online Criminal Harms Act 2023 (the OCH Act).[77] The Online Safety (Miscellaneous Amendments) Act 2022 amends the Broadcasting Act 1994[78] by imposing legal duties on social media platforms. There are two main duties. First, social media platforms with significant impact must comply with Codes of Practice. Secondly, the Infocomm Media Development Authority (IMDA) can demand social media platforms to disable access or stop the 'egregious content'

[70] Sam Stockwell, Georgia Wake, Tooska Dargahi, Oluwaseun Ajao, Annabel Latham, Ahmed Danladi Abdullahi and Dan Sexton, 'Privacy-preserving Moderation of Illegal Online Content' (April 2025), The Alan Turing Institute, 14-15, https://cetas.turing.ac.uk/sites/default/files/2025-04/cetas_research_report_-_privacy-preserving_moderation_of_illegal_online_content_0.pdf.
[71] Google uses a watermarking tool called SynthID Text. It helps developers to spot AI generated content: Geneva Internet Platform, Digwatch, 'Google unveils open-source watermark for AI text' (24 October 2024), https://dig.watch/updates/google-unveils-open-source-watermark-for-ai-text.
[72] Islamic terrorists often write in Arabic on platforms, because they are aware that content moderators working for the online platforms rarely have Arabic language skills: Tom Simonite, "Facebook is Everywhere; Its Moderation is Nowhere Close," WIRED, 25 October 2021, https://www.wired.com/story/facebooks-global-reach-exceeds-linguistic-grasp/.
[73] See 'IWF Annual Data & Insights Report 2024', https://www.iwf.org.uk/annual-data-insights-report-2024/.
[74] Stockwell et al. (n 70).
[75] See https://sso.agc.gov.sg/Bills-Supp/29-2024/Published/20240909?DocDate=20240909.
[76] See https://sso.agc.gov.sg/Acts-Supp/38-2022/Published/20221221?DocDate=20221221#top.
[77] See https://sso.agc.gov.sg/Acts-Supp/24-2023/Published/20230807.
[78] See https://sso.agc.gov.sg/Act/BA1994.

being transmitted to users.[79] 'Egregious content' broadly covers sexual content, child abuse and terrorist content but does not refer to financial scams.

The OCH Act covers a range of offences, including scams and malicious cyber activity offences under Part 2 of Schedule 1. The most notable difference between the UK Online Safety Act and the Singapore OCH Act is that the latter imposes legal duties on government officials, not online platforms. Section 3(1) of the OCH Act establishes the 'competent authority' as 'a public officer from a Ministry or department of the Government; or an employee of a public authority'. Their legal duties are then set out in section 3(2) of the OCH Act. The government can issue five types of directions under the OCH Act, namely stop communication, disabling, account restriction, access blocking, and app removal directions. A study by the IMDA in Singapore shows that online platforms are often slow to remove harmful content: on average, they take at least five days to respond to the victims.[80] This is a possible explanation of the additional role the government plays in dealing with harmful content.

Regarding scams and malicious cyber activities, the government only needs to suspect that there is online harm to issue a direction. For other activities, reasonable suspicion is required. This contrasts with the 'reasonable grounds to infer' that the content amounts to an offence in section 192(5) of the OSA 2023 for all offences including scams and cyber activities. The lower Singaporean threshold of purely suspecting there is a scam, or malicious cyber activities should make it easier to remove such content. This may be explained by the fact that Singaporeans are particularly vulnerable to scams because many of them are "affluent, digital literate and compliant".[81] Further, scam victims in Singapore suffer some of the highest losses in the world.[82]

Interestingly, a new government agency, named the Online Safety Commission, would provide faster remedies for victims.[83] Under the Online Safety (Relief and Accountability) Bill, scam victims can request perpetrators' information to commence legal proceedings.[84] They can also

[79] Part 10A of the Online Safety (Miscellaneous Amendments) Act 2022.
[80] Infocomm Media Development Authority, 'Online Safety Assessment Report 2024. Designated Social Media Services' (Singapore, 17 February 2025), p.12-13, https://www.imda.gov.sg/-/media/imda/files/regulations-and-licensing/regulations/online-safety/online-safety-assessment-report-2024-designated-social-media-services.pdf.
[81] Owen Walker, "'Rich and naive': why Singapore is engulfed in a 'scamdemic" *Financial Times* (London, 26 May 2025), https://www.ft.com/content/3299cf7e-67bd-4654-8aa9-55fc24a66b63.
[82] Infocomm Media Development Authority (n 80).
[83] See 'Singapore's Online Safety Commission: A New Era in Combatting Online Harms' (7 March 2025), https://cyberindemnity.org/2025/03/singapores-online-safety-commission-a-new-era-in-combatting-online-harms/.
[84] See https://sso.agc.gov.sg/Bills-Supp/18-2025/Published/20251015?DocDate=20251015.

sue online platforms and page administrators for deepfakes, cyberbullying and sexual harassment. Online platforms must remove offensive content alerted by users and victims. The Singapore government has also required app stores to carry out age verification through technology such as facial scans so that only users over 18 years old can use the apps.[85] These additional protections for scam victims along with the Broadcasting Act and Protection from Harassment Act 2014[86] indicate that the Singapore legislative framework adopted a strict regulatory approach to online scams.

3. The Challenges of Liability Attribution for Malicious Deepfake Scams

Establishing liability with GenAI deepfakes poses multiple challenges. Investigations are very costly and time-consuming to identify malicious content creators.[87] For example, a CEO fell victim to a deepfake video and the company detected the fraud quickly but was unable to catch the fraudster or recover financial losses.[88] Further, many deepfake investment scams involve the use of cryptocurrency. Fraudsters use deepfake videos, free cryptocurrency and promotion codes to lure victims to fake websites.[89] Once the victims enter the promotion codes, they are asked to pay Bitcoin and share their personal details, and they never got anything in return. This is particularly problematic, given that the number of generative AI enabled scams has increased by 78% in 2023-24 and then by 456% in 2024-25.[90] In the Elon Musk cryptocurrency scam of 2024, Rizzuto used a blockchain explorer and was able to trace the addresses of the scammers' wallets.[91] It was found that Bitcoin, Ethereum and Dogecoin wallets were used in

[85] Osmond Chia, "New online harms support centre to operate from 2026, will offer victims faster recourse" *The Straits Times* (8 March 2025), https://www.straitstimes.com/singapore/politics/new-online-harms-support-centre-to-begin-operation-in-2026.
[86] See https://sso.agc.gov.sg/Act/PHA2014.
[87] Bart van der Sloot and Yvette Wagensveld, 'Deepfakes: regulatory challenges for the synthetic society' (2022) 46 *Computer Law & Security Review*, p.12-13, https://doi.org/10.1016/j.clsr.2022.105716.
[88] Daniel Thomas, 'WPP boss targeted by deepfake scammers using voice clone' *Financial Times* (London, 10 May 2024), https://www.ft.com/content/308c42af-2bf8-47e4-a360-517d5391b0b0. See also Cheng Leng and Chan Ho-him, 'Arup lost $25mn in Hong Kong deepfake video conference scam' *Financial Times* (Hong Kong, 17 May 2024), https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea.
[89] Matthew D. Weiner, 'Destined to Deceive: The Need to Regulate Deepfakes with a Foreseeable Harm Standard' (2024) 122(4) *Michigan Law Review* 771, 800. It is argued that 'the intent of an individual who creates a deepfake is not debatable; certainly, after synthetically modifying an image or video, the creator did not genuinely believe that the content they shared was accurate'.
[90] See 'AI-enabled Fraud: How Scammers Are Exploiting Generative AI' (7 May 2025), TRM Blog, https://www.trmlabs.com/resources/blog/ai-enabled-fraud-how-scammers-are-exploiting-generative-ai.
[91] Rizzuto (n 53).

the scam and new wallets were used to hide the transactions. Yet, such cryptocurrency platforms are currently unregulated which results in shielded liability to scam victims.

3.1 Liability on Deepfake Content Creators

Content creators who use deepfakes to defraud victims should *in theory* bear responsibility for their crimes. Malicious content creators have the intention to mislead others and are using AI technology as a weapon to cause harm. As Mirsky and Lee posit, 'for deepfakes, the objective of the generated content is to fool a human'.[92] In the UK, there is a gap in legislation to hold malicious content creators liable. As mentioned in section 2, deepfake scams are intended harms which involve monitoring misuse by users and governing malfunction, whilst unintended harms concern rectifying design defects in AI outputs. Deepfake scam victims will need to rely on existing UK criminal legislation such as section 2 of the Fraud Act 2006 (fraud by false representation) as a potential cause of action. However, gathering clear evidence of intent to deceive by the deepfake content creators can be very challenging.

If a liability framework is to be created, we submit that the focus should be on holding them liable for failing to implement verification or safeguard measures such as disclaimers as to how much content has been altered.[93] The challenge though, is that many of such content creators are anonymous because of their nefarious activities. There are significant cost and jurisdictional barriers in uncovering the identity of these anonymous content creators.

Law enforcement techniques in the form of metadata analysis,[94] network traffic analysis,[95] financial trails[96] and behavioural analysis[97] can all assist to uncover the identity of the content creator. Courts can also issue search warrants for electronic devices to enter and search premises for evidence of serious offences under section 8 of the Police and Criminal Evidence

[92] Yisroel Mirsky and Wenke Lee, 'The Creation and Detection of Deepfakes: A Survey' (2020) 1(1) *ACM Computing Surveys*, https://doi.org/10.1145/3425780.
[93] Felipe Romero-Moreno, 'Deepfake detection in generative AI: A legal framework proposal to protect human rights' (2025) 58 *Computer Law & Security Review*, https://doi.org/10.1016/j.clsr.2025.106162.
[94] Samuele Mombelli, James R. Lyle and Frank Breitinger, 'FAIRness in digital forensics datasets' metadata – and how to improve it' (2024) 48 *Forensic Science International: Digital Investigation* 301681.
[95] Pascal Tippe and Adrian Tippe, 'Onion Services in the Wild: A Study of Deanonymization Attacks' (2024) 4 *Proceedings on Privacy Enhancing Technologies* 291.
[96] Sarah Meiklejohn et al, 'A fistful of bitcoins: characterizing payments among men with no names' (2016) 59(4) *Communications of the ACM* 86.
[97] Efstathios Stamatatos, 'A Survey of Modern Authorship Attribution Methods' (2009) 60(3) *Journal of the American Society for Information Science and Technology* 538.

Act 1984.[98] Metadata analysis of Ross Ulbricht's Gmail address and financial investigation by the Federal Bureau of Investigation led to the successful prosecution of Ulbricht, the mastermind behind the Silk Road online black market.[99] This case involved Ulbricht selling illegal drugs worth $214 million, of which 95% of the drugs were illegal.[100] He disguised his identity by using the username Dread Pirate Roberts. The scale of the operation was unprecedented, with buyers and sellers from all over the world.[101] Although the US law enforcement agencies do not disclose the costs of investigations generally, the Silk Road case involved multiple federal agencies, complex digital forensic work and a three-week federal trial.[102] Thus, it would have been a very expensive investigation. The Silk Road case was of a huge scale and led to drug related deaths. Not every case will justify the significant investigative costs. Therefore, imposing liability on content creators poses real challenges.

3.2 The Interaction between Content Creators and Online Social Media Platforms

Online social media platforms adopt GenAI technologies into their product offerings to enhance content creation workflows and empower content creators. For example, ChatGPT and Copilot are AI-powered software trained using large language models (LLMs). They are designed to assist developers in generating text through automated programming interfaces which analyse data patterns without human direction.[103] Companies largely embed generative AI models into their digital systems as they are strategic tools for creator platforms for improving user engagement, enhancing content quality, and supporting creators with limited resources or technical expertise.[104] However, the interactions between content creators and online social media platforms raise concerns about the employment of GenAI technologies to

[98] See https://www.legislation.gov.uk/ukpga/1984/60/contents.
[99] US Department of Justice, 'Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced In Manhattan Federal Court To Life In Prison' (2015), https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison.
[100] Preet Bharara and Serrin Turner, 'Government Sentencing Submission United States v. Ross William Ulbricht, 14 Cr. 68 (KBF)' (U.S. Department of Justice, 26 May 2015), https://i.brayden.id.au/gov.uscourts.nysd.422824.256.0.pdf.
[101] *United States v. Ross William Ulbricht*, 14 Cr. 68 (KBF).
[102] US Department of Justice, 'Former Silk Road Task Force Agent Pleads Guilty to Extortion, Money Laundering and Obstruction' (2015), https://www.justice.gov/archives/opa/pr/former-silk-road-task-force-agent-pleads-guilty-extortion-money-laundering-and-obstruction#:~:text=A%20former%20DEA%20agent%20pleaded%20guilty%20today%20to,and%20sale%20of%20illegal%20drugs%20and%20other%20contraband.
[103] Noam Kolt, 'Algorithmic Black Swans' (2024) 101(4) *Washington University Law Review* 1177.
[104] Di Yuan, Manmohan Aseri, Vibhanshu Abhishek and Kartik Hosanagar, 'Generative AI Adoption by Creator Platforms' (2025), The Wharton School Research Paper, p.4, https://ssrn.com/abstract=5107730.

produce reliable outputs.[105] GenAI could significantly improve creators' productivity and enhance the platform's profitability. When both creators operate on the online social media platform and choose to use AI, the quality of content improves, thereby facilitating economic returns for the platform. As noted, 'platforms offer creators visibility, enabling them to attract and engage audiences. In turn, platforms sell a share of this attention to advertisers'.[106]

The social media platform captures GenAI's potential to boost creators' productivity while maintaining their incentives to participate in content creation.[107] The issue of AI-generated deepfake financial scams has been of widespread concern for investors and consumers; more sophisticated AI tools promote scams that cause harm on online social media platforms rather than protecting vulnerable customers from worthless investment schemes.[108] GenAI's ability to catalyse deceptive or fraudulent content may reflect the appetite of big tech companies (e.g., Meta, Google, Apple, Microsoft) to publish misleading advertisements enabled by scammers in view of substantial revenues. This agent relationship identifies a potential collusive behaviour between content creators and online social media platforms, which can inflate misinformation and individuals' vulnerability to deception. It also supports Nash and Felton's argument that legislation should focus more on regulating online social media platforms as *systems* rather than just hosts of content.[109]

It is generally considered that online social media platforms provide the environment in which creators publish content and offer important monitoring capabilities for community management.[110] These platforms provide analytics tools that enable creators to measure their activities although it is questioned how to control content creation, advertising strategies and user response. This can raise concerns about the platform's responsibility for detecting, flagging, and removing harmful content to protect users and ensure trust in the distribution of information.[111] Social media companies have often been shielded from responsibility on the

---

[105] Anna Yamaoka-Enkerlin, 'Disrupting Disinformation: Deepfakes and the Law' (2020) 22(3) *New York University Journal of Legislation and Public Policy* 725.
[106] Alexander Bleier, Beth L. Fossen and Michal Shapira, 'On the role of social media platforms in the creator economy' (2024) 41(3) *International Journal of Research in Marketing* 411, 419.
[107] Nic Fildes, 'Meta sued by Australian regulator for allegedly 'misleading' crypto ads' *Financial Times* (Sydney, 18 March 2022), https://www.ft.com/content/132c7877-bd74-4957-925b-414f12ec6aa4.
[108] Jeannie Marie Paterson, 'Banks, Authorised Push Payment Scams and Models for Compensation' (2025) 99(2) *Australian Law Journal* 178, 182.
[109] Nash and Felton (n 47) 820.
[110] Noor Johnson, Matthew L Druckenmiller, Finn Danielsen and Peter L Pulsifer, 'The Use of Digital Platforms for Community-Based Monitoring' (2021) 71(5) *BioScience* 452.
[111] Miriam C Buiten, Alexandre de Streel and Martin Peitz, 'Rethinking liability rules for online hosting platforms' (2020) 28(2) *International Journal of Law and Information Technology* 139.

assumption that they constitute innovative technologies and speech platforms, such that imposing restrictions on them would amount to a form of censorship of technological progress.[112] Doctrinal debates have questioned whether social media platforms exercise their own freedom of expression rights in the course of content moderation decisions.[113]

Section 230 of the US Communications Decency Act 1996 protects technology companies from legal claims arising from user-generated content on their platforms, treating them as neutral hosts—similar to telephone companies—rather than as publishers.[114] While US legislation affords immunity to platforms for removing offensive content, courts have begun recognising causes of action that address the weaknesses and risks of social media.[115] Section 230 provides that an entity is shielded from liability only in its capacity as a provider of an interactive computer service. However, the provision does not protect a company when acting as the publisher or speaker of information provided by another information content provider.[116] As a result, a service provider is not shielded from liability where it makes a material contribution to the creation or development of content.[117] It is worth noting that GenAI outputs are not protected by Section 230, thereby undermining any defence available to companies. When a platform incorporates GenAI applications into features such as messaging and profile creation, it may jeopardise its Section 230 protection.[118] Lawsuits against social media platforms have been successful on the grounds of users' mental health harms, as illustrated by the cases *State of New Mexico v. Meta Platforms, Inc.*[119] and *K.G.M. v. Meta Platforms et al.*,[120]

---

[112] Tim Wu, 'Social Media Isn't Just Speech. It's Also a Defective, Hazardous Product' *The New York Times* (14 March 2026), https://www.nytimes.com/2026/03/14/opinion/social-media-trial-addiction.html.

[113] Stefan Theil, 'Private censorship and structural dominance: Why social media platforms should have obligations to their users under freedom of expression' (2022) 81(3) *Cambridge Law Journal* 650.

[114] Beatrice Nolan, 'Section 230 protected social media companies from legal responsibility for misinformation. AI chatbots could be about to change that' *Fortune* (8 October 2025), https://fortune.com/2025/10/08/ai-chatbot-section-230-meta-social-media-legal-shield-no-protection/.

[115] *Forrest v. Meta Platforms, LLC*, 2024 WL 3024642 (N.D. Cal. June 17, 2024). For an overview see Ryan Calo, 'Courts Should Hold Social Media Accountable — But Not By Ignoring Federal Law' (10 September 2024), *Harvard Law Review Blog Essay*, https://harvardlawreview.org/blog/2024/09/courts-should-hold-social-media-accountable-but-not-by-ignoring-federal-law/.

[116] *Forrest v. Meta Platforms, LLC*, 2024 WL 3024642 (N.D. Cal. June 17, 2024).

[117] *Rigsby v. Godaddy Inc.*, 59 F.4th 998 (9th Cir. 2023).

[118] Eric Goldman, 'Section 230 Doesn't Apply to Generative AI Enhancements to Ad Copy (But the Plaintiffs Lose Anyway)–Bouck and Suddeth v. Meta' (13 June 2026), *Technology & Marketing Law Blog*, https://blog.ericgoldman.org/archives/2026/06/section-230-doesnt-apply-to-generative-ai-enhancements-to-ad-copy-but-the-plaintiffs-lose-anyway-bouck-and-suddeth-v-meta.htm.

[119] *State of New Mexico v. Meta Platforms, Inc.*, D-101-CV-2023-02838, https://nmdoj.gov/press-release/new-mexico-department-of-justice-wins-landmark-verdict-against-meta/.

[120] *P. F., et al. (K.G.M.) v. Meta Platforms, Inc., et al.* (4:25-cv-02691), https://unicourt.com/case/ca-la23-casear4963fd3e29da-1055787.

where courts have focused on how technology platforms design their products and services to protect users from misleading or harmful content.

The EU AI Act attempts to address accountability gaps between providers and deployers. Providers are responsible for the design and documentation of AI systems, while deployers manage their contextual use and oversight. For general-purpose AI and foundation models (e.g. chatbots), upstream obligations focus on technical documentation, systemic risk mitigation, and downstream information flows, recognising their infrastructural role beyond single use cases. However, these foundation models pose significant challenges for regulators and policymakers, as they can be adapted to sophisticated automated tasks—such as those enabled by large language models—which make it difficult to detect malicious scams and to allocate responsibility.[121] Article 50 of the AI Act regulates transparency obligations for providers and deployers of certain AI systems, requiring the provision of specific information about the content and outputs of the AI system. In general terms, providers of high-risk AI systems are required to adopt additional precautions and safety measures to mitigate the undesirable effects of unexpected outcomes.[122] These obligations are complemented by the Code of Practice on the transparency of AI-generated content, which sets out regulatory measures—whose adoption is voluntary—for providers and deployers of GenAI systems on how to comply with the requirements of the AI Act.[123] Risk management requirements cover predictable and reasonably foreseeable harms associated with the use of AI applications, although sophisticated computational systems may fall outside the taxonomy introduced by the Act. Application layers deployed on AI systems generate new risks within the value chain, raising questions as to the need to examine the broader network, as the plausibility of models cannot serve as a blanket justification for assigning responsibility.[124]

Article 25 of the AI Act classifies distributors, importers, deployers, or other third parties as providers of a high-risk AI system, thereby prescribing responsibilities along the value chain. This provision must be read in conjunction with Article 16 of the Act, which sets out specific obligations for the product manufacturer as the provider of the system, focusing on the

[121] Ian Brown, 'Allocating accountability in AI supply chains: a UK-centred regulatory perspective' (June 2023) Ada Lovelace Institute, p.41, https://www.adalovelaceinstitute.org/resource/ai-supply-chains/.
[122] Michael Veale and João Pedro Quintais, 'The Obligations of Providers of General-Purpose AI Models' in Gianclaudio Malgieri, Gloria González Fuster, Alessandro Mantelero and Gabriela Zanfir-Fortuna (eds), *The EU Artificial Intelligence Act. A Thematic Commentary* (Oxford: Hart Bloomsbury 2026) ch.22.
[123] See https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content.
[124] Alessio Azzutti, 'AI Governance in Algorithmic Trading: Some Regulatory Insights from the EU AI Act' (2024) 41(1) *Banking and Finance Law Review* 133.

disclosure of information concerning the tools, services, components, and processes used or integrated within a high-risk AI system. Specifically, Article 16 establishes a capillary set of requirements to ensure compliance with the applicable conformity assessment procedures, including a series of control mechanisms related to the quality management system. Furthermore, Article 17 of the Act requires providers of AI systems to implement techniques, validation procedures, testing, examination, and systematic measures for the design, development, and data governance of the system. At first sight, the bulk of obligations placed on providers suggests that the legislation identifies them as the primary point of reference for allocating responsibility. However, unforeseen events—particularly where developers ought reasonably to have known of the existence of a risk prior to its materialisation—complicate this allocation.[125]

The perpetrator or attacker feeding adversarial data and poisoning AI provide an account of unforeseen risks which may jeopardise the attribution of responsibilities and the grounds of duties that arise in relation to the associated actions necessary to prevent the negative consequences of such events. On this point, the doctrinal debate questioned how to identify AI providers' duties for determining accountability in the AI risk management and risk assessment.[126] Unintended consequences of unforeseen outcomes are context-based, spanning predictive analysis and decision-making processes across various stages of specific AI services (e.g. machine learning, cloud computing, and GenAI applications). These dynamics significantly affect the control mechanisms governing AI systems and may shift the role of providers in relation to customer-facing application functionality.[127]

The adoption of safety measures and the ability to foresee certain risks are key to allocating liability along the AI value chain, although the level of participation of each actor, their expertise in identifying harmful effects of defective products, and the design of the AI model may alter the distribution of responsibility. As argued, 'the manufacturers of key AI components, such as foundation model providers, may be best positioned to adopt safety measures and foresee certain risks and thus should be held liable, or jointly liable, when harm

[125] Mitchell Chervu Johnston and Brian Matejek, 'Overcoming Unforeseeable AI Errors: A Proposal' (2026). Boston College Law School Legal Studies Research Paper No. 675, http://dx.doi.org/10.2139/ssrn.6344559.
[126] Ellen Hohma, 'On the elements and implications of accountability for AI providers' in Christoph Lütge, Alexander Kriebitz, Raphael Max and Caitlin C. Corrigan (eds), *The Elgar Companion to Applied AI Ethics* (Cheltenham: Edward Elgar 2024) 25.
[127] Jennifer Cobbe and Jatinder Singh, 'Artificial intelligence as a service: Legal responsibilities, liabilities, and policy challenges' (2021) 42 *Computer Law & Security Review*, https://doi.org/10.1016/j.clsr.2021.105573.

is caused by an AI system'.[128] Foundation models constitute a primary source of deepfake scams, as they are susceptible to data manipulation (such as generative content) and cyberattacks by downstream developers. Articles 53 and 55 of the EU AI Act impose obligations on providers of general-purpose AI models to disclose information concerning the training and testing processes, as well as the results of their evaluation, and require the adoption of codes of practice aimed at mitigating systemic risks originating from upstream developers. However, deepfake financial scams also raise concerns in relation to downstream developers, where modifications of foundation models by other actors within the AI value chain may generate unforeseen harms that render safety measures ineffective.[129]

Downstream activities are difficult to detect within large datasets, given the ability of third-party developers—such as those operating through application programming interfaces (APIs)—to conceal their identity when fine-tuning the original model.[130] Attributing responsibility and situating accountability to AI providers and digital platform operators for downstream harms may therefore constitute an arduous exercise, requiring a careful assessment of causation, foreseeable consequences, and applicable standards of reasonable care, which EU legislation has not yet fully addressed.[131] Imposing risk management requirements, together with a set of duties of care, skill, and diligence for senior board members of companies deploying AI models, may represent a viable option for allocating responsibility, although specific harms—such as errors in downstream activity—remain difficult to foresee.[132] Establishing a causal link between downstream activity and defective outputs requires a meticulous inquiry into whether the actors involved in the value chain possessed a sufficiently high level of expertise at a given stage of the process, as well as into the specific patterns derived from training datasets.

---

[128] Beatriz Botero Arcila, 'AI Liability Along the Value Chain: Lessons from the Liability of Suppliers of Components in Product Liability Law' (2025) 18(1) *Journal of Tort Law* 280-281.
[129] Sophie Williams, Jonas Schuett and Markus Anderljung, 'On Regulating Downstream AI Developers' (2026) 17(1) *European Journal of Risk Regulation* 103, doi:10.1017/err.2025.10020.
[130] Philipp Hacker, Ramayya Krishnan and Marco Mauer, 'Global AI Governance—Part 1: Decoding Developers and Deployers' (9 December 2024) Oxford Business Law Blog, https://blogs.law.ox.ac.uk/oblb/blog-post/2024/12/global-ai-governance-part-1-decoding-developers-and-deployers.
[131] Martin Ebers and Emmanuel Vargas Penagos, 'Upstream, downstream, and in between: navigating the GPAI value chain under EU law' (2026) *Information & Communications Technology Law*, https://doi.org/10.1080/13600834.2026.2624923.
[132] Henry L. Fraser and Nicolas P. Suzor, 'Locating fault for AI harms: a systems theory of foreseeability, reasonable care and causal responsibility in the AI value chain' (2025) 17(1) *Law, Innovation and Technology* 103, 111.

We argue that a shared liability framework can shed light on the technical complexities that the AI value chain presents in determining liability associated with fraudulent behaviour. Such a framework may operate as a deterrent mechanism by targeting each actor's contribution across the system lifecycle, thereby facilitating the foreseeability of risks and addressing regulatory gaps in the EU AI Act, which remains largely silent on how to allocate accountability for harm between upstream and downstream developers. However, a shared liability regime must be assessed on a contextual basis, and it may open the floodgates to users' compensation claims, given the incentive to seek redress from multiple parties.[133]

The idea of moral sense and self-restraint on the part of AI creators should not preclude the adoption of online regulations aimed at preventing the dissemination of misleading and fraudulent information.[134] Such regulations should not remain confined to the national level; rather, there is a need for a global consensus on how AI systems are assessed and managed, and on how liability is allocated in determining losses. However, as argued, the effectiveness of online regulation depends on the extent to which users can circumvent restrictions or substitute non-compliant platforms.[135] Creators know how to profit from their content, while users increasingly perceive platforms as providers of valuable goods and services, enabling them both to consume content and to engage in shopping activities. However, this interaction may give rise to a pernicious cycle, whereby creators are incentivised to maximise income generation and platforms, in turn, promote user engagement to accommodate creators' demand for more predictable remuneration from content-based advertising.[136]

3.3 Online Social Media Platforms' Responsibility for Deepfake Scams

Sophisticated adverts, including AI-generated deepfakes of audio and videos, persuade individuals to disclose personal data or invest in fraudulent schemes. Online social media platforms are the favourite conduit to profit from carrying the adverts and big tech companies

[133] On a similar view see Bart Custers, Henning Lahmann and Benjamyn I. Scott, 'From liability gaps to liability overlaps: shared responsibilities and fiduciary duties in AI and other complex technologies' (2025) 40(5) *AI & Society* 4035, 4043.
[134] On this point see the editorial of Martin Wolf, 'We have to manage the AI revolution' *Financial Times* (London, 17 June 2026), https://www.ft.com/content/59024744-50bf-43f7-9d79-738deabc7a60?syn-25a6b1a6=1.
[135] Matthew Brown, Emily J. Davis and Devin G. Pope, 'Can Online Activity Be Regulated? Evidence from Adult Websites' (June 2026) NBER Working Paper 35322, https://www.nber.org/papers/w35322.
[136] Catalina Goanta, 'The New Social Media: Contracts, Consumers, and Chaos' (2023) 108 *Iowa Law Review Online* 118.

seem unable to stop the number of deepfakes.[137] According to the US Federal Trade Commission Consumer Advice Report, 'scammers use social media platforms to promote bogus investment opportunities, and even to connect with people directly as supposed friends to encourage them to invest'.[138] Frauds originating on social media (e.g., Facebook, Instagram) indicate that platforms are the main method of contact and cryptocurrency is the most used method of payment.[139] We focus on regulated social media platforms such as Facebook and Instagram; largely unregulated platforms (such as Telegram, Signal, WhatsApp)[140] are outside the scope of our analysis. Public regulators and policymakers call for action to protect consumers as fraud causes severe harm to individuals and the stolen money goes to serious organised crime groups mostly hidden in the crypto platforms.[141]

Technology frauds urge more collaboration between the public and private sectors, and a 'systemic' solution is required as scammers adopt new methods and increase unauthorised losses which exacerbate a systemic problem.[142] Online social media platforms should bear a legal duty to check investment advertisers are authorised, and a legal duty not to provide advert space to fraudsters in the first place. They ought to be expected to 'know their customers' and be held liable, with proper enforcement and tough penalties, if they fail to block the dissemination of fraudulent advert content.[143] Further, online social media platforms should be legally required to check that an advertiser is authorised by a regulator to sell financial services

[137] OECD, 'Protecting Consumers from Financial Scams and Frauds' (16 June 2026), p.16-17, https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/06/protecting-consumers-from-financial-scams-and-frauds_3887b249/d41817bb-en.pdf.
[138] Emma Fletcher, 'Social media a gold mine for scammers in 2021' (January 2022), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021.
[139] See 'FTC Action Ends Ecommerce Empire Builders Online Business Opportunity Scam' (9 May 2025), https://www.ftc.gov/news-events/news/press-releases/2025/05/ftc-action-ends-ecommerce-empire-builders-online-business-opportunity-scam; 'FTC Takes Action to Stop Sprawling 'Growth Cave' Business Opportunity and Credit Repair Scam' (7 March 2025), https://www.ftc.gov/news-events/news/press-releases/2025/03/ftc-takes-action-stop-sprawling-growth-cave-business-opportunity-credit-repair-scam; 'FTC Announces Crackdown on Deceptive AI Claims and Schemes' (25 September 2024), https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes.
[140] Jacob Gursky and Samuel Woolley, 'Countering Disinformation and Protecting Democratic Communication on Encrypted Messaging Applications' (June 2021), The Brookings Institution of Foreign Policy, https://www.brookings.edu/articles/countering-disinformation-and-protecting-democratic-communication-on-encrypted-messaging-applications/.
[141] Joshua Oliver, 'The lawless world of crypto scams' *Financial Times* (London, 19 September 2022), https://www.ft.com/content/5987649e-9345-4eae-a4b8-9bfb0142a2ab.
[142] Maisie Grice, 'UK fraud 'blight' prompts calls for action to protect consumers' *Financial Times* (London, 27 May 2025), https://www.ft.com/content/c877784c-f416-4c7b-943b-dfb35a01233c.
[143] See the editorial 'How to block the financial scammers on social media' *Financial Times* (London, 18 May 2025), https://www.ft.com/content/93d29681-c242-4d0f-9789-41dbbebea906.

and block them in case there is not.[144] A mandatory risk assessment for providers of very large online platforms about the dissemination of manipulative content through their services is required by Article 34(1) of the EU DSA 2022, although this is not equivalent to an obligation to control the use of the platform, but it seems more like a due diligence test which could result in a ticking-the-box exercise.[145] This solution would not solve the problem of which party should be liable for the harm done by such frauds, but the fact that sellers of financial products must usually be registered with regulators would incentivise to blocking of a particularly harmful online fraud.

Court rulings have begun to recognise the responsibility of technology companies in cases where they fail to control the products and services they place on the digital market. A German regional court found Google liable for false claims (including scams, links to dubious companies, subscription traps, and suspicious phone calls) and inaccurate information contained in an AI-generated search overview, which was treated as its own content rather than merely as a list of search results.[146] The court made clear that Google has influence over the AI's offering and the algorithms with which the AI operates, which essentially convert the function of generative search from a hosting service to a publishing service.[147] Another interesting case is the UK's Competition and Markets Authority (CMA) action against Google under the Digital Markets, Competition and Consumers Act 2024.[148] The CMA imposed targeted rules on Google's search services following its decision to designate the company as having Strategic Market Status (i.e. market power combined with a position of strategic significance in a digital activity) in the provision of general search services.[149] This designation allows the CMA to introduce conduct requirements governing Google's search activities,

[144] Akila Quinio and Martin Arnold, 'Social media must do more to tackle payment fraud, says UK regulator' *Financial Times* (London, 14 October 2024), https://www.ft.com/content/1e77ae86-a0c2-47ee-804b-cbe50765a9a8.
[145] Stefano Faraoni, 'Why Generative AI Is Not Cyrano de Bergerac. A Computational Manipulation Perspective on Generative AI' in Mimi Zou, Cristina Poncibò, Martin Ebers and Ryan Calo (eds), *The Cambridge Handbook of Generative AI and the Law* (Cambridge: Cambridge University Press 2025) 56.
[146] Regional Court of Munich (Landgericht Muenchen I), temporary injunction in case no. 26 O 869/26, https://cdn.arstechnica.net/wp-content/uploads/2026/06/Google-AI-Overview-Munich-Court-Ruling.pdf.
[147] Foo Yun Chee, 'Google to challenge German ruling saying it is liable for AI-generated false claims' (12 June 2026), *Reuters*, https://www.reuters.com/world/google-appeal-german-court-ruling-assigning-liability-ai-overviews-false-claims-2026-06-12/.
[148] Competition and Markets Authority, 'CMA secures fairer deal for publishers and improves Google search services in UK' (3 June 2026), Press Release, https://www.gov.uk/government/news/cma-secures-fairer-deal-for-publishers-and-improves-google-search-services-in-uk.
[149] Reuters, 'Google must let UK publishers opt out of AI search under new rules' (3 June 2026), https://www.reuters.com/legal/litigation/uk-regulator-enforces-new-competition-requirements-google-search-2026-06-03/.

provided that such measures are proportionate to the objectives of ensuring fair dealing, open choices, and trust and transparency.[150]

We argue that a regulatory framework imposing shared responsibility for deepfake financial scams on malicious content creators and online social media platforms would provide a viable redress mechanism for victims' losses and would impose corresponding obligations on these actors to compensate those affected by fraud. Such a solution may be particularly appropriate where a content creator intentionally trains an AI model to produce deceptive outputs, and where online platforms use such outputs to distort or manipulate information—rather than to moderate or report harmful content—relevant to individuals' decision-making processes.[151]

4. The Conundrum of a Liability Regime in GenAI

The liability contours of deepfakes financial scams involve multiple actors at multilevel stages of GenAI: malicious deepfake content creators, software developers, and online social media platforms. Regulatory challenges around the liability degree for malicious scams have raised concerns on the suitable remedies and normative interventions.[152] Most disputes allocate the responsibility to consumers for reasonable care in their decision-making process following the principle of 'caveat emptor'.[153] However, this approach does not resolve the issue of liability attribution for unforeseeable harms, which could not be reasonably prevented, such as inaccurate outputs generated by AI tools embedded in GenAI and LLMs[154] that 'hallucinate'

[150] Competition and Markets Authority, 'Further CMA action to secure a fairer deal for businesses and improve Google search services in UK' (17 June 2026), Press Release, https://www.gov.uk/government/news/further-cma-action-to-secure-a-fairer-deal-for-businesses-and-improve-google-search-services-in-uk.

[151] Peter Henderson, 'Challenges for Foundation Model Liability and Regulatory Regimes. An Analysis of US Law' in Mimi Zou, Cristina Poncibò, Martin Ebers and Ryan Calo (eds), *The Cambridge Handbook of Generative AI and the Law* (Cambridge: Cambridge University Press 2025) 126-127.

[152] Judit Bayer, 'Legal implications of using generative AI in the media' (2024) 33(3) *Information & Communications Technology Law* 310.

[153] In *Santander UK Plc v CCP Graduate School Ltd* [2025] EWHC 667 (KB), the court held that a bank may reasonably foresee harm to innocent third parties once alerted to the fact that one of its accounts has been used by fraudsters; however, it did not have a relationship with such third parties sufficient to establish the necessary proximity. This decision reflects the approach adopted by the Supreme Court in *Philipp v Barclays Bank UK plc* [2023] UKSC 25, where a bank customer was the victim of authorised push payment fraud and had been deceived into instructing the bank to transfer funds to fraudsters. In *Royal Bank of Scotland International Ltd (Respondent) v JP SPC 4* [2022] UKPC 18, the Privy Council had accepted that the bank "had no special level of control over the source of danger (i.e., it was not in control of the fraudsters)".

[154] LLMs are computational deep learning models trained on an immense quantity of data, capable of understanding and generating natural language to perform a wide range of tasks. An analysis of "hallucinations" in the LLM outputs is conducted by Claudio Novelli, Luciano Floridi, Stefan Larsson, Mariarosaria Taddeo and Steven L. Winter, 'The Artificial in "Artificial Intelligence": How Imagination Shapes AI Regulation' (2026), p.30-31, https://philarchive.org/archive/NOVTAI-2v2.

users with fabricated or false information about historical events, legal filings, news and research articles.[155] AI hallucinations produce plausible but incorrect outputs, even with perfect data, due to fundamental statistical and computational limits which cause unintentional errors in the decision-making process.[156] The datasets used to train the models can be biased, inaccurate or intentionally disrupted by content creators who provide faulty narratives to manipulate information.[157] As argued, corrupted data and information make GenAI outputs no longer so intelligent, profitable, or socially beneficial for market participants.[158] However, GenAI hallucinations not only produces false outputs but are entangled in the cognitive experience (e.g., memories, emotions, behaviour) that characterises the human-AI interaction in conversational interfaces.[159] GenAI tools hallucinate because the training and evaluation procedures reward guessing over acknowledging uncertainty: AI models do not acknowledge

[155] Hallucinated outputs in GenAI result from training data, the design of tools focused on pattern-based content generation, and the inherent limitations of AI models. See MIT Management, 'When AI Gets It Wrong: Addressing AI Hallucinations and Bias' (2026), https://mitsloanedtech.mit.edu/ai/basics/addressing-ai-hallucinations-and-bias/.
In *Tajudin bin Gulam Rasul v Suriaya bte Haja Mohideen* [2025] SGHCR 33, the Singapore Court ordered the claimant's counsel personally to pay costs to the defendant for having cited a fictitious authority in the claimant's written submissions. The hallucinated case was created by GenAI and spotted by the defendant's counsel. Claimant's counsel omitted the hallucinated case from the bundle and subsequently sought to file a revised version of the submissions with a replacement authority without the Court's permission. Claimant's counsel provided the explanation that the hallucinated case had been unintentionally cited. Claimant's counsel also sought to explain the revised submissions as merely "to update the document due to typographical errors without any amendments to the contents" and to correct "clerical errors". The defendant's counsel was willing to accept the claimant's counsel's representations and that the hallucinated case might have been unintentionally cited. The Court considered that claimant's counsel's conduct was, amongst other things, improper. The Court noted that "of gravest concern, [claimant's counsel] was less than candid with the Court and sought to downplay the gravity of his improper conduct". The decision sets out a multi-factor approach to determine the egregious nature of counsel's misuse of GenAI and how costs should be apportioned as a result. The decision holds: (a) whether the fictitious AI-generated authority was intentionally cited to mislead or deceive the court; (b) whether the advocate and solicitor had previously cited fictitious AI-generated authorities to the court; (c) whether an immediate, full and truthful explanation is given to the court and the counterparty. Specifically, whether the advocate and solicitor expeditiously informed the court that a fictitious AI-generated authority was cited and took appropriate steps, in consultation with the court, to remedy the mistake, or conversely, if he displayed a lack of candour and attempted to downplay or conceal his mistake; and (d) the impact on the underlying litigation, in particular, whether the legal proposition purportedly supported by the fictitious authority exists and could have been supported by a genuine authority [at para 72].
[156] It has been reported that epistemic uncertainty arises when information appears rarely in training data, that model limitations occur where tasks exceed the representational capacity of current architectures, and that computational intractability persists where even superintelligent systems cannot solve cryptographically hard problems. See Adam Tauman Kalai, Ofir Nachum, Santosh S. Vempala and Edwin Zhang, 'Why Language Models Hallucinate' (2025), https://arxiv.org/pdf/2509.04664.
[157] Naja Bentzen, 'Information manipulation in the age of generative artificial intelligence' (December 2025), European Parliamentary Research Service PE 779.259,
https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/779259/EPRS_BRI(2025)779259_EN.pdf.
[158] Tom C.W. Lin, 'Artificial Intelligence, Misinformation, and Market Misconduct' (2024) 85(4) *Ohio State Law Journal* 685, 702.
[159] Lucy Osler, 'Hallucinating with AI: Distributed Delusions and "AI Psychosis"' (2026) 39(1) *Philosophy & Technology*, https://doi.org/10.1007/s13347-026-01034-3.

uncertainty, they provide estimates as facts without deeper research about the validation of their statements.[160] The impact of uncertainty about the performance of GenAI is a matter of concern for legal practice and consumer claims disputes, where the large use of AI models poses risks of misperception in accessing valuable advisory assistance.[161] There is a pressing need to address the harmful impact of outcomes due to the uncertainty and unpredictability of risks in the GenAI supply chain.[162] AI risk frameworks have proved inadequate for the reality of persistent hallucinations; they often underestimate epistemic uncertainty, so updates are needed to address systemic unpredictability.[163] In the doctrinal debate, it has been noted that additional concerns result from the lack of a universally accepted definition of hallucinations.[164] As a result, there is no reliable way of measuring their occurrence and evaluating the reliability of specific GenAI-based tools. Requiring disclosure or certification of GenAI use—such as a mandatory 'hyperlink rule'[165] in legal citations and contentions to authoritative sources—would mitigate the users' reliance to hallucinated cases through verification at the point of citation.[166]

Situations of unintended harms caused by faulty outputs (e.g., hallucinating critical information in providing advice or assistance as a result of genuinely defective AI behaviour) are distinct from intentional abuse of a dual-use technology to commit fraud (e.g., human-generated misinformation in influencing decision-making). Human misinformation is technically and

[160] In *R (Ayinde) v London Borough of Haringey* [2025] EWHC 1383, hallucinated cases, or "fake authorities," were regarded as professional misconduct. The Court held that "placing false material before the court with the intention that the court treats it as genuine may, depending on the person's state of knowledge, amount to a contempt. That is because it deliberately interferes with the administration of justice" [at para 26]. The Court recognised that "the information produced by generative large language model artificial intelligence tools is a result of their operational design. They generate textual responses by predicting what words or phrases come next in a particular context, based on patterns identified from a vast quantity of training data" [at para 6].

[161] Vivi Tan, Jeannie Marie Paterson and Julian Webb, 'Generative Artificial Intelligence in Small Value Consumer Claims: Hallucination Risk, System Design, and Governance in Online Dispute Resolution' (2025) 48(4) *University of New South Wales Law Journal*, 1277.

[162] Teresa Rodríguez de Las Heras Ballell, 'Mapping Generative AI rules and liability scenarios in the AI Act, and in the proposed EU liability rules for AI liability' (2025) 1 *Cambridge Forum on AI: Law and Governance* 7.

[163] Gyana Swain, 'OpenAI admits AI hallucinations are mathematically inevitable, not just engineering flaws' (18 September 2025), https://www.computerworld.com/article/4059383/openai-admits-ai-hallucinations-are-mathematically-inevitable-not-just-engineering-flaws.html?trk=feed_main-feed-card_feed-article-content.

[164] Eliza Mik, 'Revisiting Legal Hallucinations' (10 March 2026), Centre for Legal Innovation and Digital Society (CLINDS)'s 30th LegalTech Seminar, Faculty of Law, The Chinese University of Hong Kong.

[165] An electronic link embedded in a citation that allows direct access to the cited authority would refrain the careless use of AI outputs.

[166] Oliver Roberts, 'Spread of AI Hallucinations Drives Need for Sanctions Reporting' (20 February 2026) Bloomberg Law, https://news.bloomberglaw.com/legal-exchange-insights-and-commentary/spread-of-ai-hallucinations-drives-need-for-sanctions-reporting.

conceptually different from AI hallucinations in terms of motivations, beliefs, and intent.[167] This results in human-initiated inaccuracies which involve deliberate deception or flawed prompts, leading to disinformation as intentional falsehoods and computational manipulation of individuals' choice.[168] As a corollary, intentional misuse of GenAI may exacerbate the risk of deteriorating the information ecosystem with lower-quality, synthetic, or misleading content, effectively generating untruthful content.[169] Sophisticated forms of market manipulation come from misuse of AI techniques such as algorithmic trading which faces 'challenges to guaranteeing accountability and assigning responsibility, as human experts do not explicitly program the AI behaviour'.[170] The complexity and interoperability of automated trading practices as well as their autonomy in the decision-making activity (self-learning from own experience from the observation of markets) make difficult to identify the liability degree (among the parties involved in designing, developing, using, and monitoring the AI system) for misconduct and harm when operating in financial transactions. An innovative proposal to implement a credible deterrence regulatory framework to achieve effective law enforcement of securities law has been suggested in the doctrinal debate with a view to address unlawful behaviours and conduct in the trading context.[171]

Manipulated content in deepfake financial scams undermines technological advancements and exploits vulnerabilities of software design in facilitating intentional fraud, misinformation and emotional harm.[172] The Financial Stability Board (FSB) warned about the potential of GenAI to increase financial fraud and the ability of malicious actors to generate and spread disinformation in financial markets, which urges the need for accountability mechanisms and content moderation.[173] Generative AI visual text is produced by a human designer or creator,

---

[167] Anqi Shao, 'New sources of inaccuracy? A conceptual framework for studying AI hallucinations' (2025) 6(4) *Harvard Kennedy School Misinformation Review*, 3.
[168] Stefano Faraoni, 'AI-Enabled Manipulative Techniques: A Contract Law Perspective' (2026) *Lloyd's Maritime and Commercial Law Quarterly* 77.
[169] Joseph E. Stiglitz and Maxim Ventura-Bolet, 'The Impact of AI and Digital Platforms on the Information Ecosystem' (October 2025) NBER Working Paper Series No. 34318, p.3-4, http://www.nber.org/papers/w34318.
[170] Alessio Azzutti, 'AI trading and the limits of EU law enforcement in deterring market manipulation' (2022) 45 *Computer Law & Security Review* 4.
[171] Ibid., 12-13. It is noted that such a regulatory framework is workable if it guarantees detection, prosecution, and sanctioning of misconduct. This proposal is complemented with a multi-layered liability framework for AI trading manipulation, which integrates administrative and criminal liability aspects relating to AI misconduct to ensure preventive detection of unlawful activities and collaboration in information disclosure and enforcement action with the regulatory authorities.
[172] David Hirshleifer et al., 'AI, Opinion Ecosystems, and Finance' (February 2026), NBER Working Paper Series No. 34807, http://www.nber.org/papers/w34807.
[173] FSB, 'The Financial Stability Implications of Artificial Intelligence' (14 November 2024), p.2, https://www.fsb.org/uploads/P14112024.pdf

adapted to representational media for altering users' beliefs, and distributed to mislead the audience.[174] It is human fault to deceive and distort the reality through materials artificially created by the AI tool; this affects market structure and trading exchanges with negative implications on competition and transaction costs.[175] When AI tools self-learn and self-operate with disrupted data to achieve an unlawful objective, it is difficult for regulatory authorities and market users to understand how the outputs are originated. Conduct of business rules can mitigate the risks of traders committing abuses, although the high-speed data used in financial products make monitoring and supervisory activities meaningless with respect to technological errors.[176] Risk management and internal controls within financial firms are often inadequate to detect the potential harms posed by malicious deepfake scams; in parallel, regulatory compliance frameworks and prudential standards adopted by financial authorities exhibit weaknesses in terms of skills and resources (including deficiencies in data science expertise and essential IT capabilities) necessary to assess AI tools.[177] Model validation, ongoing monitoring, outcome analysis, and data quality assessment entail substantial compliance costs and require a thorough understanding of the vulnerabilities associated with AI models. This, in turn, calls for the development of policy frameworks that enhance engagement with private sector participants, AI developers, and other third-party service providers.[178]

4.1 The Shared Liability Model

We identify different scenarios for allocating responsibility among parties implicated in fraudulent AI-generated outcomes. We contend that a shared liability regime would provide a legal response to fraudulent content, as well as act as a deterrent by discouraging malicious

---

[174] Michael D. Murray, 'Visual Legal Rhetoric in the Age of Generative AI and Deepfakes: Renaissance or Dark Ages?' (2025) 28(1) *SMU Science and Technology Law Review* 199, 230-231.

[175] Chinmayi Sharma, 'AI's Hippocratic Oath' (2025) 102(4) *Washington University Law Review* 1101, 1159-1160, where it is proposed a new professional licensing process for artificial intelligence engineers.

[176] Yesha Yadav, 'Oversight Failure in Securities Markets' (2019) 104(7) *Cornell Law Review* 1799, 1855. It is pointed out that "the likelihood of error and disruption is amplified by ineffective oversight in fragmented markets {…} which can be addressed by introducing mutual contribution to a compensatory fund to pay out on liability claims when a single exchanges or dark pool cannot" (at 1858). A system of shared liability fund for trading venues can reduce incentives for market participants to take risks that cannot cover in case of losses, and can facilitate industry self-monitoring and discipline.

[177] FSB, 'Enhancing Third-Party Risk Management and Oversight. A toolkit for financial institutions and financial authorities' (4 December 2023), p.33, https://www.fsb.org/uploads/P041223-1.pdf.

[178] OECD, 'Regulatory approaches to Artificial Intelligence in finance' (September 2024), OECD Artificial Intelligence Papers No. 24, p.35-36, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/09/regulatory-approaches-to-artificial-intelligence-in-finance_43d082c3/f1498c02-en.pdf.

content creators and online social media platforms from disseminating deepfakes. This approach originates in the broader debate concerning the conceptual framework of single liability shared among multiple injurers.[179] The shared responsibility applies to multiple stakeholders proportionally responsible for a particular action or outcome.[180] The share of liability must be assessed on a case-by-case basis depending on the duty carried by each party involved in the illegal activity. The limitations of this proposed liability approach lie in the potential hurdles in identifying the specific harm associated with the deceptive action for each party involved in the AI supply chain. These limitations reflect the risk of misallocating the burden of responsibility among the actors engaged in the system lifecycle, thereby both diluting accountability in the decision-making process and placing disproportionate compliance burdens on AI providers.

Andhov and Gardner observed that complex algorithmic decision-making systems challenge the application of tort law as an appropriate private cause of action to ensure compensation for individual victims of financial harm.[181] Specifically, it could be difficult to demonstrate that the fault of the algorithm caused the harm experienced. In the context of the tort of negligence, it is observed that risks of harm can be reasonably foreseeable, and the exact causal mechanism of the harm does not need to be reasonably foreseeable.[182] Howells and Twigg-Flesner proposed a liability approach that allows the user to seek redress without having to face the difficulties associated with identifying the correct party responsible.[183] Ben-Shahar offers a suggestive view on fault-based liability in tort law and apportionment problems by proposing a safety score liability which is commensurate with a party's habitual propensity to behave unsafely.[184] This proposal is based on measurable and predictable persons' actions identified by a machine learning algorithm score calculation to determine the probability of causing accidents with occurred harms.[185] The implementation of safety score liability would be suitable for assessing

[179] Anna Beckers and Gunther Teubner, 'Responsibility for Algorithmic Misconduct: Unity or Fragmentation of Liability Regimes?' (2023) 25(Special Issue) *Yale Journal of Law and Technology* 76, 94-95.
[180] Bart Custers, Henning Lahmann and Benjamyn I. Scott, 'From liability gaps to liability overlaps: shared responsibilities and fiduciary duties in AI and other complex technologies' (2025) 40(5) *AI & Society* 4035.
[181] Alexandra Andhov and Jodi Gardner, 'Duties of Care for Algorithmic Decision-Making in the Financial Industry', paper presented at the NUS Law and Fintech Conference, Singapore, 31 July-1 August 2025.
[182] On this discussion see Law Commission, 'AI and the Law' (31 July 2025), Discussion Paper, p.11, https://lawcom.gov.uk/publication/artificial-intelligence-and-the-law-a-discussion-paper/.
[183] Geraint Howells and Christian Twigg-Flesner, 'Interconnectivity and Liability. AI and the Internet of Things' in Larry A. DiMatteo, Cristina Poncibò and Michel Cannarsa (eds), *The Cambridge Handbook of Artificial Intelligence* (Cambridge: Cambridge University Press 2022) 198.
[184] Omri Ben-Shahar, 'Safety Score Liability' (2025) 17(1) *Journal of Legal Analysis* 190..
[185] This regime proposes that parties are partially liable in proportion to their safety score, as it has been noted, 'the higher the safety score, the lower the fraction of liability'. Ibid., 196.

the responsibility of content creators and software developers, although the algorithmic system that calculates the scores should be trained with accurate data on the parties involved, which may prove difficult in the case of anonymous malicious deepfake scammers. Some commentators found limitations of liability law pointing out that is 'too blunt an instrument for allocating responsibility to meet society's needs, and that any attempt to improve that allocation via law and regulation needs to focus on the implementation of appropriate governance systems by GenAI supply chain members and also to recognise that risk prevention is an impossible target, instead focusing on mitigation of risks to a socially acceptable level'.[186]

We situate the shared liability regime on causation in tort law to identify responsible actors in the deepfake network among multiple causes of the same injury which arises in negligence and results from significant, foreseeable, and harmful risks.[187] This regime allows the identification of the burden of responsibility for manipulating the GenAI system across the supply chain while providing consumers effective remedies to claim compensation where fraudulent practices compromise their decision-making process. However, the proportion of responsibility as articulated in the shared liability regime may find limitations to protect reasonable expectations of safety and reliability in AI software from an average consumer.[188] Practical implementation of the shared liability is examined in the party's actions to heighten the risk of faulty outcomes. The more fundamental problem is identifying certain actors at all—especially given limited enforcement resources, anonymity, and cross-border operations. These real-world constraints are essential to any feasible liability model.

Our proposal for a shared liability regime advances existing debates on the development of a more resilient AI risk framework, in which all parties are required to implement more robust verification technologies and protocols to protect consumers. In cases where victims are scammed, a shared liability regime would provide guidance on the allocation of liability among the relevant parties.

---

[186] Chris Reed and Keri Grieman, 'Responsibility for generative AI services – from aspiration to achievement' (2025), p.7-8, https://ssrn.com/abstract=5107667.

[187] Richard W. Wright, 'Allocating Liability among Multiple Responsible Causes: A Principled Defense of Joint and Several Liability for Actual Harm and Risk Exposure' (1988) 21(4) *U.C. Davis Law Review* 1141. See also Omri Ben-Shahar, 'Causation and Foreseeability' in Gerrit De Geest (ed), *Encyclopedia of Law and Economics*, vol. 1, *Tort Law and Economics* (2nd edn., Cheltenham: Edward Elgar 2009) ch.3.

[188] Geraint Howells, 'Protecting Consumer Protection Values in the Fourth Industrial Revolution' (2020) 43(1) *Journal of Consumer Policy* 160; Peter Cartwright, 'Understanding and Protecting Vulnerable Financial Consumers' (2015) 38(2) *Journal of Consumer Policy* 119, 127.

4.2 Liability for Deepfake Software Developers

The missing party being held liable in the deepfake scam supply chain is deepfake software developers, which can be used for legitimate and even beneficial purposes. This makes it difficult to impose blanket liability on all deepfake software developers. We consider the scenario of liability for creating software engineering in which developers hold responsibility for using methodologies which may be manipulated for harmful deepfake content (e.g., audio, visual images, advice). Developers of automated tools such as agentic integrated development environments (LLMs such as GitHub and Copilot X) can generate code programming to support human skills.[189] Software development methodologies require ongoing monitoring, adaptation and refinement to avoid hacking and data leakage which gives access to fraudster content creators.[190] Developers can provide safeguards to the software to refrain hackers and malicious users from accommodating requests of cyberattacks. Although the safeguards can be eluded by a downstream user, a few proactive techniques can be adopted to monitor users performing harmful tasks, such as open-sourcing, stress-test models pre-release, structured model access for third-party auditors and research APIs to facilitate external independent model evaluation.[191] These defensive strategies can be implemented by creating a group of 'red-team professionals' to provide effective safety evaluations of AI models.[192]

The shared liability regime can be implemented for developers based on the tort of negligence for failure to ensure due care in ensuring the safety and reliability of the software (generated code and automation) as well as providing software updates. Developers should be responsible for the code review and debugging of software, although they often bargain with the online platforms, agreeing to distribute exclusivity through big tech companies in exchange for reduced fees.[193] This is in line with Article 50 of the EU AI Act which places a number of

[189] Marijn Janssen, 'Responsible governance of generative AI: conceptualizing GenAI as complex adaptive systems' (2025) 44(1) *Policy and Society* 45-46.
[190] Tim Howard, 'GenAI and software development: a new paradigm' (2 June 2025), Blog Defra digital, data, technology and security, https://defradigital.blog.gov.uk/2025/06/02/genai-and-software-development-a-new-paradigm/.
[191] Elizabeth Seger et al., 'Open-Sourcing Highly Capable Foundation Models: An evaluation of risks, benefits, and alternative methods for pursuing open-source objectives' (2023) *Computers and Society*, p.17, https://doi.org/10.48550/arXiv.2311.09227.
[192] Red-team and research API solutions aim to foster transparency in the AI model while enhancing collaborative and multi-stakeholder efforts to evaluate the model components. See Chinmayi Sharma, 'Concentrated Digital Markets, Restrictive APIs, and the Fight for Internet Interoperability' (2019) 50(2) *University of Memphis Law Review* 441, 451-452.
[193] Fiona M. Scott Morton, *Digital Platform Regulation: Making Markets Work for People* (Yale School of Management 2025) 135.

obligations on providers and users of AI systems to enable the detection and tracing of AI-generated content.[194]

An interesting case of accountability regime is found in medical law where software has been interpreted as a service rather than a product, on account of a fault liability for the injury that occurred from the integration of AI systems into healthcare practice, which is shared between physicians, hospitals and product developers.[195] The EU Product Liability Directive (PLD)[196] includes software as a product for the purposes of a no-fault liability, reframing it under the strict liability regime.[197] This impact is that producers of software can be held responsible for damage caused by their defective products, regardless of fault.[198] In the academic debate, it is argued that software have become important elements of products and were even remotely interconnected with them.[199] Therefore, the case for considering software like any other component have become stronger with the result that the producer of the software itself could be liable in their own capacity whether as supplier of software as a component or as standalone software. On this view, it is observed that 'as AI is more pervasive and ubiquitous – just like other software – it might soon be found in a significant number of consumer products and services'.[200] However, the definition of software as a product remains cryptic in the PLD as it

[194] Mar Negreiro, 'Scam calls in times of generative AI' (October 2025), European Parliamentary Research Service PE 777.940,
https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/777940/EPRS_ATA(2025)777940_EN.pdf.
[195] Regulation (EU) 2017/745. See also W. Nicholson Price II, Sara Gerke and I. Glenn Cohen, 'Liability for use of artificial intelligence in medicine' in Barry Solaiman and I. Glenn Cohen (eds), *Research Handbook on Health, AI and the Law* (Cheltenham: Edward Elgar 2024) 166.
[196] Directive (EU) 2024/2853.
[197] Article 4(1) of the PLD. It is worth noting that, at the UK level, the Law Commission has embarked on a review of the legislation on liability for defective products. This review aims to update and substantially reform UK legislation, which dates back to the mid-1980s and was enacted as Part I of the Consumer Protection Act 1987, itself based on the EU Product Liability Directive adopted in 1985. Since then, a much wider range of products has emerged, particularly as a result of digitalisation. A large number of physical products now incorporate software, and many have the capability to connect to the internet or other networks. Furthermore, a wide array of digital products has developed in the form of applications and AI-based systems; however, none of these currently falls within the scope of existing product liability legislation in the UK.
On this discussion see https://lawcom.gov.uk/project/product-liability/.
[198] Recital 2 of the PLD indicates that "liability without fault on the part of economic operators remains the sole means of adequately addressing the problem of fair apportionment of risk inherent in modern technological production". Recital 13 makes clear that "software is a product for the purposes of applying no-fault liability, irrespective of the mode of its supply or usage, and therefore irrespective of whether the software is stored on a device, accessed through a communication network or cloud technologies, or supplied through a software-as-a-service model".
[199] Christian Twigg-Flesner and Geraint Howells, 'Adapting Consumer Law to New Technologies' in Roger Brownsword and Larry A. Di Matteo (eds), *The Cambridge Handbook of the Governance of Technology* (Cambridge: Cambridge University Press 2026) 160.
[200] Przemysław Pałka and Agnieszka Jabłonowska, 'Consumer law and artificial intelligence' in Woodrow Barfield and Ugo Pagallo (eds), *Research Handbook on the Law of Artificial Intelligence* (2nd edn., Cheltenham: Edward Elgar 2025) 591.

is not clear whether digital content with equivalent functions and software as a service are included in the scope of the revised product category.[201] Specifically, the Directive does not provide a clear demarcation between the concept of software-as-a-service (e.g., computer programs and AI systems) and software as a genuine digital service (e.g., digital offerings) when it is treated as a product in its own right. Recital 13 of the PLD provides some indication that software may be considered either as a standalone product or as integrated into other products as a component; however, it does not distinguish between 'software' and 'service', nor does it classify genuine digital services as related services (e.g., the supply of data), which are de facto excluded from the category of products.[202]

Software is capable of causing damage through its execution, and manufacturers should remain liable for defectiveness as a result of related services within their control.[203] As Howells and Twigg-Flessner observe, the term 'producer' is given a broad meaning under the PLD.[204] It goes beyond the manufacturer, and can include even the producer of raw components; the manufacturer of components and even importers of the products. We posit that deepfake software producers would fall within the PLD and therefore can be accountable to any victims' losses.[205]

Article 12 of the PLD states that multiple economic operators can be held liable jointly and severally for the same damage; the liability is not reduced where the damage is caused both by the defectiveness of a product and by an act or omission of a third party.[206] Responsibility for testing of high-risk AI systems is placed under Article 60(9) of the EU AI Act, which requires

---

[201] Teresa Rodriguez de las Heras Ballel, 'Civil liability and artificial intelligence : challenges, policy options and legal responses' in Woodrow Barfield and Ugo Pagallo (eds), *Research Handbook on the Law of Artificial Intelligence* (2nd edn., Cheltenham: Edward Elgar 2025) 482.
[202] European Law Institute, 'Liability for Defective Software Under the New EU Product Liability Regime. Will Liability Under the New PLD Extend to Social Media, AI Chatbots and Similar Digital Consumer Offerings?' (22 June 2026) 1st Supplement to the ELI Draft of a Revised Product Liability Directive, p.14-15, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Liability_for_Defective_Software_Under_the_New_EU_Product_Liability_Regime.pdf.
[203] Recital 50 of the PLD.
[204] Howells and Twigg-Flessner (n 183) 186-187.
[205] An example of software leading to significant damages in finance is the errors committed by Knight Capital Americas LLC in 2012. Its defective computer software led to the router sending four million orders into the market to fill just 212 customer orders. The Securities Exchange Commission held that Knight Capital failed to have adequate safeguards in place to limit the risks posed by its access to the markets; to prevent the entry of millions of erroneous orders, and to adequately the effectiveness of its controls. Strict liability however, may hinder innovation and deepfake software has dual purposes. Arash Massoudi, 'Knight Capital glitch loss hits $461m' *Financial Times* (London, 17 October 2012), https://www.ft.com/content/928a1528-1859-11e2-80e9-00144feabdc0. US Securities and Exchange Commission, 'SEC Charges Knight Capital With Violations of Market Access Rule (U.S., 28 July 2014), https://www.sec.gov/newsroom/press-releases/2013-222.
[206] Article 13 of the PLD.

that ‘providers should be held liable for any damage caused in the course of their testing in real world conditions’. Limitations of the shared liability framework of the PLD emerge in relation to financial harms caused by faulty algorithmic procedures, which require an effective right to compensation and a redress scheme. Specifically, the shared liability approach may fail to capture responsibility for immaterial harms (e.g., discriminatory outputs, breaches of privacy, emotional losses), which necessitate enforcement mechanisms capable of awarding damages for defective products.[207]

Prevention measures to refrain malicious actors also include government certification programme and authorisation schemes for assessing the software before running onto the platforms.[208] The licence regime would test the used technology to ascertain that the software components (e.g., operating system, code and data)[209] are aligned with the requirements of safety and reliability. On this view, it has been noted that ‘regulators should only grant such licenses if applicants can show that the use of generative AI will provide consumers with financial guidance that is at least as accurate and well-tailored as the guidance that is provided by more conventional symbolic AI’.[210] The rapid development of face-swapping AI technology questioned how to identify the scam and how to measure the deepfake.[211] The capacity for face-swapping to deceive is bolstered by voice-cloning applications; the voice changing device raises concerns for its use in various operations such as buying a product on the platform or creating voices and cloning them.[212] The significant challenge is that face-swapping can be used for commercial purposes but can also be used for malicious investment fraud, although the question is, how can the licencing system work when the AI software can be used for both purposes? Proper safeguard measures such as regulatory requirements and compliance methods can be imposed on the software developer in order to detect the characteristics and purpose of

[207] Sandra Wachter, ‘Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond’ (2024) 26(3) *Yale Journal of Law & Technology* 671, 704.
[208] Anuragini Shirish and Shobana Komal, ‘A Socio-Legal Inquiry on Deepfakes’ (2024) 54(2) *California Western International Law Journal* 555-556.
[209] A software component is defined as “a unit of composition with contractually specified interfaces and explicit context dependencies only. A software component can be deployed independently and is subject to composition by third parties”. See Clemens Szyperski et al., *Component Software: Beyond Object-Oriented Programming* (2nd edn., Boston: Addison-Wesley Pearson Education 2002) ch.1.
[210] Daniel Schwarcz, Tom Baker and Kyle Logue, ‘Regulating Robo-Advisors in an Age of Generative Artificial Intelligence’ (2025) 82(1) *Washington & Lee Law Review* 775, 806.
[211] Yi Yan, ‘Deep Dive into Deepfakes—Safeguarding Our Digital Identity’ (2023) 48(2) *Brooklyn Journal of International Law* 768.
[212] Liam James, ‘Face-swapping: Why you can’t trust a video call – and how scammers are taking advantage’ *Independent* (28 February 2025), https://www.independent.co.uk/tech/deepfake-scam-face-swap-fraud-ai-b2706722.html.

synthetic media distribution, and the identification of natural persons through fingerprint information.[213] It has been noted that policy intervention should focus on the sociotechnical domain, such as the identification of content manipulations through authentication practices to verify the accuracy of the source of content and preserve the distribution chain.[214]

The Australian Scams Prevention Framework Act 2025 requires digital platforms to check all advertisers of financial products have an Australian Financial Services Licence and take specific steps in the verification of new accounts.[215] Along with these preventive regulatory tools, tech companies have developed trial processes such as regulatory and digital sandboxes to mitigate the risks of harmful outcomes of AI models. The European Council defined regulatory sandboxes as:

'concrete frameworks which, by providing a structured context for experimentation, enable where appropriate in a real-world environment the testing of innovative technologies, products, services or approaches […] for a limited time and in a limited part of a sector or area under regulatory supervision ensuring that appropriate safeguards are in place'.[216]

Regulatory sandboxes such as digital 'scale up box' can be implemented to monitor the quality and performance of GenAI applications.[217] These regulatory tools launched by the FCA to test Fintech products are designed to establish a safe environment to oversee technological software and foster innovation.[218] They aim to enhance cooperation between regulatory authorities and

[213] Momina Masood, Mariam Nawaz, Khalid Mahmood Malik, Ali Javed and Aun Irtaza, 'Deepfakes Generation and Detection: State-of-the-art, open challenges, countermeasures, and way forward' (2023) 53(4) *Applied Intelligence*, 4013-4014.

[214] Ellen P. Goodman, 'Synthetic Content: Default to Distrust' (2025) Rutgers Law School Research Paper, p.27, https://ssrn.com/abstract=5236368. It is argued that 'defaulting to authentic content and requiring labelling for synthetic content would put the burden on those who want to authenticate content or provide provenance information for synthetic content'.

[215] Australian Government The Treasury, 'Scams Prevention Framework. Protecting Australians from scams' (3 February 2025), p.5, https://treasury.gov.au/publication/p2025-623966.

[216] Council Conclusions on Regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age (16 November 2020), 13026/20, https://data.consilium.europa.eu/doc/document/ST-13026-2020-INIT/en/pdf.

[217] Walter G. Johnson, 'Caught in quicksand? Compliance and legitimacy challenges in using regulatory sandboxes to manage emerging technologies' (2023) 17(3) *Regulation & Governance* 709.

[218] See https://www.fca.org.uk/firms/innovation/regulatory-sandbox. The FCA launched a Supercharged Sandbox tool using NVIDIA accelerated computing and NVIDIA AI Enterprise Software to provide firms access to better data, technical expertise and regulatory support to test AI systems. The Supercharged Sandbox aims to support innovative, early-stage AI projects in financial services. See 'FCA allows firms to experiment with AI alongside NVIDIA' (9 June 2025), https://www.fca.org.uk/news/press-releases/fca-allows-firms-experiment-ai-alongside-nvidia; https://fcainnovation.co.uk/wp-content/uploads/2025/06/supercharged-sandbox-participation-pack.pdf.

financial firms with a view to promoting best practices for transparency of the automated systems.

An innovative regulatory approach against the risks of unexpected outcomes of technology applications is the FCA's consumer duty which concerns the firm's conduct in relation to financial services.[219] The consumer duty rule sets the standard of care that firms should give to customers in retail markets and holds responsible manufacturers and distributors for the assessment of foreseeable harms.[220] The duty applies across the distribution chain such as the design or operation of products or services and the firm's responsibilities depend on its role and ability to influence retail customer outcomes.[221] Manufacturers are required to monitor the characteristics of their products and whether are fit for purpose, and distributors are under obligation to have a clear understanding of the target market and the way products operate.[222] Software developers and digital platforms are expected to use watermarking techniques to deploy reliable content authentication and provenance mechanisms to enable users to identify AI-generated content.[223] Firms need to share information about harmful content of technological applications with other relevant parties, in particular where a distributor identifies foreseeable harm or problems with the way a product or service is operating in practice.[224] The consumer duty can impose a main obligation for firms to report fraudulent

[219] FCA, 'Final non-Handbook Guidance for firms on the Consumer Duty' (July 2022), FG22/5, p.35, https://www.fca.org.uk/publication/finalised-guidance/fg22-5.pdf. It is stated that 'where a firm is planning to alter or withdraw a product or service, they should consider whether it could lead to foreseeable harm for their customers or a specific group of customers (such as customers with characteristics of vulnerability) and take steps to mitigate the impact of the potential harm'.

[220] Iris H.-Y. Chiu and Wai-Yee Wan, 'Constructing a Taxonomy of Financial Consumer Protection Policy and Assessing the New Consumer Duty in the United Kingdom's Financial Sector' (2024) 7(2) *Cardozo International & Comparative Law Review* 465.

[221] The duty applies in the distribution chain, including the manufacture, provision, sale and ongoing administration and management of a product or service to the end retail customer. Under the consumer duty, firms are required to assess, test, understand and evidence the types of products and services that they offer. A firm is not required to go beyond its role in the distribution chain nor monitor or take responsibility for a separate firm's compliance. See Robin Henry and Abbie Coleman, 'Could there be consumer duty failure claims within your distribution chain?' *Financial Times* (London, 11 October 2023), https://www.ftadviser.com/regulation/2023/10/11/could-there-be-consumer-duty-failure-claims-within-your-distribution-chain/.

[222] Manufacturers and distributors need to identify foreseeable harms where products or services were poorly designed or were distributed widely to customers for whom they were not designed.

[223] Watermarking tools are used for content authentication, data monitoring, indicating authorship and protecting copyright. See Tambiama Madiega, 'Generative AI and watermarking' (December 2023), European Parliamentary Research Service PE 757.583, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)757583.

[224] Manufacturer firms need to inform distributors of the characteristics of a product or service, its target market and the value it is intended to provide to customers and, to support manufacturers reviewing a product or service, distributors need to provide relevant information to them. Firms are responsible only for their own activities and are not required to oversee the actions of other firms in the distribution chain; however, they may be held

behaviours in deepfake scams relating to GenAI products and implement internal controls to detect potential harmful software.[225] The FCA duty rule can be implemented by firms to reduce vulnerability of GenAI tools although compliance requirements, such as risk management processes and transparency obligations, may not be effective in detecting (and avoiding) potential harmful outputs.[226] Further, the consumer duty rule requires firms to conduct an assessment of the AI model and its use and operation before deploying outcomes to the market.[227]

4.3 Risk Management and Verification Measures for Deepfake Software Developers and Online Social Media Platforms

We argue that deepfake software companies and online social media platforms should be held liable for negligence if they do not adequately implement risk management processes and verification measures to prevent harmful misuse such as deepfake scams, although we acknowledge that these solutions may prove ineffective to capture on time the unintended malicious actions of users. It is expected that software developers should use biometric and identity verification to prevent unauthorised use of someone's likeness by requiring consent verification before processing images or voice samples of identifiable individuals. Watermarking techniques such as hashing are forgery methods to check the integrity of content by tracing files with a short string of numbers that is lost if the video or audio is deepfaked.[228] Failure to employ digital forensic techniques in GenAI amounts to gross negligence, which

---

responsible in certain circumstances for the actions of other parties where they exercise material influence over customer outcomes.
See https://www.fca.org.uk/publications/good-and-poor-practice/consumer-duty-implementation-good-practice-and-areas-improvement; https://www.fca.org.uk/firms/consumer-duty-information-firms.

[225] FCA, 'Immediate areas for action and further plans for reviewing FCA requirements following introduction of the Consumer Duty' (March 2025), Feedback Statement FS25/2, https://www.fca.org.uk/publication/feedback/fs25-2.pdf.

[226] Teresa Rodríguez de Las Heras Ballell, 'Mapping Generative AI Liability Cases in the EU Legal Framework' in Mimi Zou, Cristina Poncibò, Martin Ebers and Ryan Calo (eds), *The Cambridge Handbook of Generative AI and the Law* (Cambridge: Cambridge University Press 2025) 106.

[227] FCA, 'FCA helps firms to test AI safely' (December 2025), https://www.fca.org.uk/news/press-releases/fca-helps-firms-test-ai-safely; 'Our Consumer Duty focus areas' (May 2026), https://www.fca.org.uk/publications/corporate-documents/consumer-duty-focus-areas; 'Consumer Duty implementation: good practice and areas for improvement' (December 2025), https://www.fca.org.uk/publications/good-and-poor-practice/consumer-duty-implementation-good-practice-and-areas-improvement.

[228] Liam Kearns, Abu Alam, Jordan Allison, 'Synthetic Media Authentication Threats: Detection using a Combination of Neural Network and Blockchain Technology' (2025) 36(8) *Transactions on Emerging Telecommunications Technologies* e70225.

results in personal liability for individuals accountable for careless supervision of content authenticity.[229] Digital forensic techniques employ blockchain technology which can verify the origins and distribution of videos by storing digital signatures in a ledger which is difficult to manipulate.[230]

The UK Cyber Security and Resilience Bill 2024,[231] which updated the Network and Information Systems (NIS) Regulations 2018,[232] established a set of provisions that impose obligations on managed service providers (IT service providers and managed security services),[233] holding responsible those firms for failure to take effective technical and organisational measures (e.g., contractual requirements, security checks, or continuity plans) and to manage risks posed to the security of the network, infrastructure, and information systems.[234] The concept is similar to our proposal of imposing liability on those responsible for negligence. In China, Provisions on the Administration of Deep Synthesis of Internet-based Information Service 2023 introduced specific obligations and responsibilities on service providers, users and online platforms for the management of synthetic media technologies.[235] Alongside these legislative frameworks, supervisory authorities should develop response programmes tailored to address the threats posed by deepfake manipulation. These programmes would establish procedures for identifying, assessing, and mitigating the harmful consequences of malicious deepfake content, supported by regulatory tools designed to

[229] David Atkinson and Jacob Morrison, 'A Legal Risk Taxonomy for Generative Artificial Intelligence' (2024) *Computers and Society*, https://arxiv.org/pdf/2404.09479.
[230] Mika Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9(11) *Technology Innovation Management Review* 46.
[231] See https://www.gov.uk/government/collections/cyber-security-and-resilience-bill.
[232] See https://www.legislation.gov.uk/uksi/2018/506.
[233] The Bill targets managed service providers by expanding the scope of security duties imposed on digital service providers (including online marketplaces, online search engines, and cloud computing services). The term 'managed service providers' refers to the ongoing provision of management support, active administration, or monitoring of IT systems, infrastructure, applications, or networks, including activities related to cybersecurity that involve a network connection or access to the customer's network and information systems. The Bill also introduces supply chain security requirements by embedding duties relating to supply chain security for operators of essential services within the legislative framework. Senior managers and directors are responsible under the Cyber Governance Code of Practice (https://www.gov.uk/government/publications/cyber-governance-code-of-practice/cyber-governance-code-of-practice), which complements the Bill 2024 in governing cyber security risks. See the editorial 'In cyber attacks, humans can be the weakest link' *Financial Times* (London, 26 May 2025), https://www.ft.com/content/4349b16a-8ec1-44d9-a295-3a51523805a8.
[234] Jonathon Ellison, 'Cyber Security and Resilience Policy Statement to strengthen regulation of critical sectors' (1 April 2025), https://www.ncsc.gov.uk/pdfs/blog-post/cyber-security-resilience-bill-policy-statement.pdf.
[235] See https://www.pkulaw.com/en_law/90cff392df74a3ebbdfb.html. For commentary see Yinuo Geng, 'Comparing "Deepfake" Regulatory Regimes in the United States, the European Union, and China' (2023) 7(1) *Georgetown Law Technology Review* 157, 169-170.

enhance coordination between enforcement mechanisms, intelligence agencies, and other relevant stakeholders.

We submit that deepfake software developers and online social media platforms should implement risk management techniques to identify, assess, and mitigate the harmful impact of deepfake AI content. Where AI-generated content is detected but does not violate platform policies (e.g. parody), platforms should apply a prominent, immutable label (e.g. 'AI-generated' or 'Synthetic Media'), which remains visible even when the content is shared or downloaded. Furthermore, if a user receives a message containing phrases such as 'Bitcoin', 'investment opportunity', or 'send money', a pop-up alert could warn: 'Be careful. Scammers often promise guaranteed returns. Never send money to someone you have only met online.' Similarly, if a user shares a video identified as a potential deepfake scam, a warning could appear stating: 'This media has been identified as potentially synthetic. Learn more about deepfakes.'

Liability could also be imposed on software developers through implementing reasonable safeguards. For example, Microsoft launched safety benchmarks for developers to rank iterations from a range of providers in view to build trust with cloud customers.[236] The safety metric evaluates whether a model can be used for malicious purposes: this testing programme based on rankings enables users to understand the risks posed by AI applications.[237] It is an innovative mechanism to monitor GenAI products by ensuring they cannot be used to create harmful content. The safety system evaluates the level of fairness, biases and mistakes of AI products, and the risk of fraudulent hallucinated outputs in investment scams.[238]

The Singapore Government launched testing pilot schemes namely the Global AI Assurance Pilot,[239] the Joint Testing Report with Japan,[240] and the AI Safety Red Teaming Challenge

[236] Rafe Uddin and Cristina Criddle, 'Microsoft to rank 'safety' of AI models sold to cloud customers' *Financial Times* (London, 7 June 2025), https://www.ft.com/content/02f39b33-fa6e-4bb7-b1f4-8171b50738af.
[237] Liang Yu, Emil Alégroth, Panagiota Chatzipetrou and Tony Gorschek, 'Measuring the quality of generative AI systems: Mapping metrics to quality characteristics — Snowballing literature review' (2025) 186 *Information and Software Technology*, https://doi.org/10.1016/j.infsof.2025.107802.
[238] David Krause, 'Mitigating Risks for Financial Firms Using Generative AI Tools' (2023), https://ssrn.com/abstract=4452600.
[239] See https://aiverifyfoundation.sg/ai-assurance-pilot/.
[240] See https://sgaisi.sg/wp-api/wp-content/uploads/2025/03/International-Network-of-AI-Safety-Institutes-Joint-Testing-Exercise-Improving-Methodologies-for-AI-Model-Evaluations-Across-Global-Languages.pdf.

Evaluation Report[241] to enhance the best practices of GenAI governance. Red teaming requires programmes to be tested in an adversarial manner and scenario planning, with the aim of detecting malicious and manipulative actions of software developers.[242] The Monetary Authority of Singapore prescribes explicit duties for banks and telecommunications providers under the Shared Responsibility Framework, acting in coordination with the Infocomm Media Development Authority (IMDA) when allocating responsibility for losses arising from a defined scope of phishing scams.[243] The Supreme Court of Singapore has attributed liability for AI-generated content to users, thereby complementing the Shared Responsibility Framework 2024 and the Protection from Scams Act 2025.[244] In parallel, English courts have held that there is a professional duty to use AI tools "with an appropriate degree of oversight, and within a regulatory framework that ensures compliance with well-established professional and ethical standards".[245]

Under the OSA 2023, senior managers of online social media platforms may incur criminal liability if they fail to implement proportionate systems and processes designed to prevent the publication and hosting of fraudulent advertising. Within the shared liability model, we posit that, where the scale of harm justifies it—as in the Silk Road operation—content creators should also be held liable for deepfake scams. We acknowledge the challenges associated with uncovering the anonymity of content creators, which is why we have focused on the liability of software developers and online social media platforms. We further contend that deepfake software companies and online social media platforms should be held liable for negligence where they fail to adequately implement risk management processes and authentication methods designed to prevent harmful misuse, such as deepfake scams.

We suggest that online social media platforms should adopt protocol design and governance policy guidelines to prevent the harmful risks posed by AI-generated content while, in parallel, assessing user expectations as to whether the purpose of such content is to mislead or distort

---

[241] See IMDA, 'Singapore AI Safety Red Teaming Challenge' (February 2025), Evaluation Report, https://www.imda.gov.sg/-/media/imda/files/about/emerging-tech-and-research/artificial-intelligence/singapore-ai-safety-red-teaming-challenge-evaluation-report.pdf.
[242] Orly Lobel, 'The AI Regulatory Pyramid: A Taxonomy & Analysis of the Emerging Toolbox in the Global Race for the Regulation and Governance of Artificial Intelligence' (2025) 57(4) *Loyola of Los Angeles Law Review* 890-891.
[243] IMDA, 'MAS and IMDA announce implementation of Shared Responsibility Framework from 16 December 2024' (24 October 2024), https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/implementation-of-shared-responsibility-framework.
[244] See https://sso.agc.gov.sg/Acts-Supp/1-2025/Published/20250217?DocDate=20250217.
[245] *R. (on the application of Ayinde) v Haringey LBC* [2025] EWHC 1383 (Admin) [at para 5].

beliefs. Corporate governance boards (including senior management, directors, executives, and compliance officers) of software companies and online platforms should be trained and fully informed about the reputational risks that the use of defective GenAI models may pose to business operations.[246] Poor monitoring of expected outputs and a limited understanding of AI decision-making processes can lead to compliance failures and flawed corporate reporting, thereby affecting the expectations of investors and market stakeholders.

5. Conclusion

Advances in generative computing software provide firms with greater opportunities to create smarter services for customers; however, they also provide scammers, fraudsters, and creators of deepfakes with more powerful tools.[247] GenAI content can disseminate inaccurate information and unintended 'hallucinations' that are not factually reliable, and it is often difficult to trace how a particular output has been generated.[248] Malicious deepfakes operate at different stages of the AI supply chain through digital platforms, thereby complicating the identification of fraudulent activity.

The time is ripe for regulatory intervention. We proposed a shared liability regime to attribute responsibility to actors involved in the creation and dissemination of fraudulent AI-generated content. This regime would enable a more balanced approach to compensation, whereby the parties involved would bear losses proportionately, depending on whether, and to what extent, they contributed to the scam. The FCA's Consumer Duty can complement the shared liability regime by requiring firms to avoid foreseeable harm to customers arising from the behaviour of AI models. However, the UK regulatory framework does not provide adequate responses to the risks of automated manipulation of information in synthetic media, as the impersonation of individuals by scammers exacerbates unfair practices against users. This suggests that UK legislation should consider specific liability approaches that account for the timing and nature of deepfake scams, which may undermine the safety and reliability of outcomes, while also

[246] Patrick J. O'Malley, 'Generative AI Systems and Corporate Governance, Compliance and Liability. Rethinking Director and Officer Roles in Light of a New World of Technological, Legal and Ethical Challenges' in Mimi Zou, Cristina Poncibò, Martin Ebers and Ryan Calo (eds), *The Cambridge Handbook of Generative AI and the Law* (Cambridge: Cambridge University Press 2025) 369 and 382.
[247] Stephen Bush, 'Are we human or are we spammer?' *Financial Times* (London, 24 June 2025), https://www.ft.com/content/07ed552a-e681-472a-8eba-c4b3a7938027.
[248] Cristina Criddle, 'How to get the best out of AI' *Financial Times* (London, 10 June 2025), https://www.ft.com/content/d2f1fa02-025c-41ff-814f-00f22ed5c6d3.

imposing responsibility on online social media platforms to compensate victims. The normative experience of Singapore in tackling online scams and sharing the costs of fraud may offer a useful policy model for the UK Government in establishing mandatory rules for compensating losses and allocating liability among multiple parties involved in malicious deepfake activities.