

volume 36 • issue 1 • issn 0959-3799

e**ntertainment** law review

Impact of the EU AI Act on the Creative Industries

ANDREW WILSON-BUSHELL AND SOPHIE NEAL

Fashionably Dressed Down—CMA Targets Greenwashing in the Rag Trade

HELENA FRANKLIN

Balancing Innovation and Privacy: Navigating Data Protection in India's Evolving Gaming Regulation Landscape

SOUMYA PRAKASH PATRA

Comparing the Core Duty to Secure Free Speech in Higher Education Under the 1986 and 2023 Acts

JAMES MURRAY

Anti-Counterfeiting and Your Intellectual Property Rights

SIMON MILES

Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes—Ofcom Releases Discussion Paper Concerning the Harmful Impact of AI-Generated Deepfakes

STACEE SMITH

Offside! CJEU Judgment that Finds FIFA Transfer Rules Anti-competitive Set to have Major Implications for the Football Transfer Market

STEPHEN SMITH, SEAN-PAUL BRANKIN AND IVA GOBAC

Court of Appeal Considers Relevance of a Crowded Market and Earlier Coexistence Agreements in Determining Likelihood of Confusion Between "Polo Club" Brands

SARAH HUSSLEIN

National Youth Council of Moldova v Republic of Moldova: Advertising, Free Speech and the Protection of Minorities

STEVE FOSTER

FOIA Commercial Interests Exemption—First-tier Tribunal Considers British Museum's Entitlement to Withhold Information Relating to its Dealings with a Commercial Sponsor

ROHAN MASSEY

Not Such an EASYLIFE—easyGroup Unsuccessful in its Latest Trade Mark Action Challenging the Use and Registration of EASY LIVE in the United Kingdom

JOHN PATTEN, ALEX ZAPALOWSKI AND ALI FAZELI-NIA

Parish v Wikimedia Foundation Inc: Permission to Serve Out Set Aside, Forum and Merits Tests Failed, "Single Publication Rule" Applied

HUGH TOMLINSON KC

Summary Judgment Granted Against Law Firm on the Basis that it had No Real Prospect of Proving Defamatory Reviews Caused It Serious Financial Loss

MATTHEW DANDO

Journalists Beware—High Court Rules Trade Unions Can Sue for Libel

JEMMA WEBSTER

Sweet & Maxwell

EDITORIAL BOARD

editor-in-chief:

TONY MARTINO
Barrister
London

editor:

RICO CALLEJA
Calleja Consulting
London

editorial board:

PHIL ALBERSTAT
Osborne Clarke, London

ED BADEN-POWELL
Simkins LLP, London

LEONARD D. DUBOFF
The DuBoff Law Group PC
Portland, Oregon

JANE C. GINSBURG
Columbia University Law School
New York

GIOVANNI A. PEDDE
Pedde & Associates
Rome

ANTHONY M. SEDDON
Consultant Solicitor at BakerLaw LLP,
London

ERIC BARENDT
Goodman professor of Media Law
University College London

correspondents:

Advertising & marketing:
OLIVER BRAY
Partner, RPC
London

digital content:

MARIE-CLAIRE MCCARTNEY
Senior Legal Adviser, Sky
London

publishing:

Eileen Weinert
Senior Legal Counsel
Paramount

sport & media:

PATRICK MITCHELL
Partner, Latham & Watkins
London

Table of Contents

Articles

ANDREW WILSON-BUSHELL AND
SOPHIE NEAL

Impact of the EU AI Act on the Creative Industries 1

The EU's Artificial Intelligence Act came into force on 1 August 2024. It will set the tone for providers and users of AI systems in the EU, and probably globally. Its stated purpose is “to promote the uptake of human-centric and trustworthy artificial intelligence” and to make sure that “AI systems in the EU are safe, transparent, traceable, non-discriminatory and environmentally friendly”. In this article, we take a look at the parts of the Act most likely to be relevant to the creative industries and when the various requirements are set to come into force.

HELENA FRANKLIN

Fashionably Dressed Down—CMA Targets Greenwashing in the Rag Trade 6

The Competition and Markets Authority has published a bespoke guide called *Green claims in fashion*—based on its Green Claims Code—targeted at fashion businesses. The CMA is concerned that customers should be able to make informed choices based on trustworthy environmental claims. Accordingly, the guidance is tailored to increase fashion brands' compliance with consumer law and to protect shoppers from misleading claims about the green credentials of fashion brands and their products and services. It also reminds businesses of the CMA's enforcement powers (soon to be enhanced) in the event of a breach of consumer law.

SOUMYA PRAKASH PATRA

Balancing Innovation and Privacy: Navigating Data Protection in India's Evolving Gaming Regulation Landscape 10

This article explores the challenges that the gaming industry in India faces regarding legal issues on data protection and privacy in the rapidly growing sector. The article provides a critical analysis of the legal framework, the recent legislation and relevant case laws that prescribe personal data governance by gaming industry entities. The article also highlights the issues of Indian regulatory trends and compares them with action in the global arena and identifies regulatory gaps for future legislative activity emphasising user protection and innovation.

JAMES MURRAY

Comparing the Core Duty to Secure Free Speech in Higher Education Under the 1986 and 2023 Acts 14

The article will discuss the key case law which has interpreted the core s.43(1) duty on higher education providers under the Education (No.2) Act 1986 to take reasonably practicable steps to secure free speech within the law and will describe how this duty interact with universities' obligation as public authorities to act compatibly with the European Convention on Human Rights, particularly the art.10 right to freedom of expression. It will consider the claim of the Conservative Government that the Higher Education (Freedom of Speech) Act 2023 strengthened the core s.43(1) duty under the 1986 Act and, if so, to what extent.

SIMON MILES

Anti-Counterfeiting and Your Intellectual Property Rights 19

This article provides guidance for businesses dealing with intellectual property crimes or looking to safeguard their intellectual property rights against future infringements.

STACEE SMITH

Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes—Ofcom Releases Discussion Paper Concerning the Harmful Impact of AI-Generated Deepfakes 24

This article considers the issues raised in Ofcom's discussion paper titled “Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes”, published in July 2024. The paper highlights the proliferation and societal impact of deepfakes, indicates practical measures to control harms associated with deepfakes and identifies areas where the inadequacy of such measures may warrant regulatory interventions.

Comments

STEPHEN SMITH, SEAN-PAUL BRANKIN
AND IVA GOBAC

Offside! CJEU Judgment that Finds FIFA Transfer Rules Anti-competitive Set to have Major Implications for the Football Transfer Market 28

This article reviews and considers the implications of the Court of Justice of the European Union's ruling in *FIFA v BZ (Diarra)* that FIFA's rules underpinning the current multi-billion euro football transfer market contravene EU rules on free movement and competition.

SARAH HUSSLEIN

Court of Appeal Considers Relevance of a Crowded Market and Earlier Coexistence Agreements in Determining Likelihood of Confusion Between “Polo Club” Brands 32

This article examines the Court of Appeal’s ruling in *Lifestyle Equities CV v Royal County of Berkshire Polo Club*. The judgment considers how a crowded market with similar-themed brands as well as the presence of coexistence agreements, entered into by the claimant and defendant with third parties, influence the assessment of the likelihood of confusion in trade mark infringement cases.

STEVE FOSTER

National Youth Council of Moldova v Republic of Moldova: Advertising, Free Speech and the Protection of Minorities 34

National Youth Council of Moldova v Republic of Moldova examines how the European Court balances the right of free, public interest, speech with the rights of others not to be subject to hate speech or ridicule, in a case concerning the banning of a poster with cartoon representations of minority groups.

ROHAN MASSEY

FOIA Commercial Interests Exemption—First-tier Tribunal Considers British Museum’s Entitlement to Withhold Information Relating to its Dealings with a Commercial Sponsor 37

This article reviews the decision of the First-tier Tribunal in *Garrard v Information Commissioner* that the British Museum was entitled to rely on the commercial interest’s exemption in the Freedom of Information Act (FOIA) to withhold information requested of it in relation to BP’s sponsorship of the museum.

JOHN PATTEN, ALEX ZAPALOWSKI
AND ALI FAZELI-NIA

Not Such an EASYLIFE—easyGroup Unsuccessful in its Latest Trade Mark Action Challenging the Use and Registration of EASY LIVE in the United Kingdom 39

This article reviews and comments on the High Court ruling in *easyGroup Ltd v Easy Live (Services) Ltd*, one of the latest in a string of actions by easyGroup Ltd and its affiliates seeking to establish broad protection for any brand with the “easy” prefix in the UK.

HUGH TOMLINSON KC

Parish v Wikimedia Foundation Inc: Permission to Serve Out Set Aside, Forum and Merits Tests Failed, “Single Publication Rule” Applied 42

This article reviews and comments on the judgment of Steyn J in *Parish v Wikimedia Foundation* setting aside an order granting the claimant in a libel action permission to serve the defendant out of the jurisdiction.

MATTHEW DANDO

Summary Judgment Granted Against Law Firm on the Basis that it had No Real Prospect of Proving Defamatory Reviews Caused it Serious Financial Loss 44

This article reviews and comments on *BW Legal Services v Trustpilot* in which the High Court dismissed a libel claim, brought by a law firm specialising in debt recovery, against Trustpilot relating to 20 reviews posted on the platform, on the basis that the firm had no real prospect of success in proving on the balance of probabilities that each, or any, of the reviews caused, or was likely to cause, it serious financial loss for the purpose of the Defamation Act 2013 s.1.

JEMMA WEBSTER

Journalists Beware—High Court Rules Trade Unions Can Sue for Libel 45

This article reviews and comments on the High Court ruling in *Prospect v Evans* that trade unions have the right to sue in defamation and earlier authority to the contrary was wrongly decided.

Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes—Ofcom Releases Discussion Paper Concerning the Harmful Impact of AI-Generated Deepfakes

Stacee Smith

UK SOLICITOR AND BERMUDA BARRISTER

🔗 Deepfakes; Generative artificial intelligence; OFCOM

On 23 July 2024, Ofcom published a discussion paper titled “Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes”.¹ The paper highlights the proliferation and societal impact of “deepfakes”, defined in the paper as forms of audiovisual content that has been generated or manipulated using AI, which misrepresents someone or something. Deepfakes are usually intended to cause harm by deceiving an audience into believing that something happened when it did not and they do not always feature real people. Instead, they may feature an environment or a setting, and either consist of entirely new content or existing content that has been manipulated in some form.

Background

Since they are designed to be deceptive, many deepfakes are undocumented. However, studies suggest that nonconsensual intimate content is one of the most common forms of deepfakes shared online, with women (including ordinary members of the public, celebrities, politicians and other public figures) most often falling victim. Leading campaign group My Image, My Choice (MIMC) estimates that there are now over 276,000

videos of this nature circulating on the most popular deepfake sites, with over 4.2 billion total views, and many of the women featured suffer from anxiety, PTSD and suicidal ideation as a result.²

In recent months, there have been multiple high-profile incidents that have significantly increased public concern about this technology, such as the “deep nude” images of Taylor Swift that went viral on social media³ and the fake audio that purportedly depicted London Mayor Sadiq Khan criticising last year’s Armistice Day parades.⁴ Romance scams and fraudulent adverts are other forms of deepfakes that have caused problems, and as the new regulator for online safety with various services regulated under the Online Safety Act 2023 (OSA), Ofcom is committed to curtailing the circulation of malicious content.

Other efforts to mitigate the creation and spread of deepfakes include new laws and offences, such as an offence under the OSA that prohibits the sharing of deepfake intimate images.⁵ The tech industry is also taking steps to combat this issue, via watermarking schemes,⁶ tighter policies⁷ and increased use of detection and labelling tools.⁸

Although not all content created by this technology is harmful, the availability of new tools powered by Generative AI (GenAI), which allow users to create wholly new content that is significantly more convincing and life-like, has made it easier for anyone with even modest technical skills to create deepfakes. This is because, in comparison to the two original forms of AI that existed for many years—Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs)—GenAI is simpler and cheaper to use, and it has greater capability of creating more convincing content, a wider range of content creation and manipulation, and adapting to specific use cases.

The emergence of a “deepfake economy” has also led to the increase in the creation and sharing of deepfakes online, as professional creators are now offering to create deepfakes on behalf of others for a fee, user-friendly bespoke apps make it easier for people to create deepfakes and there are even websites that are dedicated to hosting deepfake content.

Harm caused by deepfakes

Ofcom outlines the manner in which deepfakes can cause harm by dividing them into three categories: those that demean, those that defraud and those that disinform.

¹ “Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes” (Ofcom, 23 July 2024).

² Deepfake Abuse: Landscape Analysis (MIMC), <https://myimagemychoice.org/fake-action/>.

³ “AI-Generated Taylor Swift Porn Went Viral on Twitter: Here’s How It Got There” (404 Media, 25 January 2024), <https://www.404media.co/ai-generated-taylor-swift-porn-twitter/>.

⁴ “Counter-terror investigation launched into deepfake of Sadiq Khan backing pro-Palestine protest on Armistice Day” LBC News, 10 November 2023, <https://www.lbc.co.uk/news/sadiq-khan-deepfake-police-investigating-pro-palestine-protest/>.

⁵ Online Safety Act 2023 s.188 inserts ss.66B, 66C and 66D into the Sexual Offences Act 2003 to create three new offences of sharing an intimate photograph or film, and one new offence of threatening to share an intimate photograph or film.

⁶ See M. Hiikkilä, “Why Big Tech’s watermarking plans are some welcome good news” (MIT Technology Review, 13 February 2024), <https://www.technologyreview.com/2024/02/13/1088103/why-big-techs-watermarking-plans-are-some-welcome-good-news/>.

⁷ See K. Paul, “Meta overhauls rules on deepfakes, other altered media” (Reuters, 5 April 2024), <https://www.reuters.com/technology/cybersecurity/meta-overhauls-rules-deepfakes-other-altered-media-2024-04-05/>.

⁸ See, e.g. J. Flannery O’Connor and E. Moxley, “Our approach to responsible AI innovation” (YouTube, 14 November 2023), <https://blog.youtube/inside-youtube/our-approach-to-responsible-ai-innovation/>.

Demean

Deepfakes that demean are created to humiliate or abuse a victim-survivor by falsely depicting them in a certain manner or performing a certain act. This content may only require a small audience (or even no audience at all, other than the victim) to have a devastating impact. For example, when intimate images are involved they can severely disrupt victim-survivors' lives by shifting their sense of self, their identity and their relationships with their bodies and others.⁹

Sometimes the threat of spreading the deepfake beyond the victim-survivor is enough to accomplish the perpetrator's goal, such as fear or extortion, and the availability of a demeaning deepfake can represent lifelong emotional and reputational harm even if the content is no longer accessible online.

Defraud

Defrauding deepfakes are mainly used to assist fraudulent behaviour such as scam communications and false advertising, but they can also facilitate other activity such as grooming. The identity of the victims is often not important to the perpetrators, as they could be focused on one person or be designed to deceive a mass audience of thousands or even millions.

A well-known example of a defrauding deepfake is the fake advert featuring Martin Lewis that was shared on Facebook, in which he appeared to be asking users to sign up for a non-existent Elon Musk investment.¹⁰

Compared with demeaning deepfakes, the "harm half-life" of a defrauding deepfake may be short, reflecting the opportunistic nature of this form of deception, but fraudulent deepfakes that have been around for days, months or years may still be effective at defrauding their targets.

Disinform

Deepfakes that disinform are mainly aimed at shaping public opinion on political and social issues, such as those relating to elections, healthcare and cultural topics. Disinforming deepfakes often aim to discredit a particular individual, such as a political candidate ahead of an election, or create controversy surrounding a particular event, such as a military conflict.

Microsoft, for instance, reported that it had observed Chinese-affiliated actors using AI to create deepfakes on politically divisive issues, including gun violence in the US.¹¹

While many disinforming deepfakes are intended to be shared as widely as possible, some are targeted at select groups of individuals or a community bound by

certain beliefs. The Global Network on Extremism and Technology (GNET) claims that synthetic audio and image content is being used by extremist networks to spread propaganda and recruit new people to their cause.¹²

Although the impact of a disinforming deepfake may diminish following a particular event, such as an election, some deepfakes in this category may be a persistent source of disruption. Deepfakes that amplify conspiracy theories or perpetuate hateful and misleading claims can have lasting impacts.

Tackling deepfakes

Ofcom has identified four broad categories of intervention which can be applied by different actors at various stages in the technology supply chain.

Prevention

Any attempt to stop a harmful deepfake from being created typically involves introducing safeguards "upstream" to limit what models can produce. Such preventative measures include model developers taking the following actions: opting to omit certain types of data from their training datasets, introducing filters that instruct a model to reject problematic prompt requests, adding output filters that automatically inspect generated content and block that which is deemed harmful, and using red teaming (a type of AI model evaluation which can help identify safety vulnerabilities) or other methods of evaluation to assess the likelihood of their model creating deepfake content.

However, preventative measures do have limitations, including the fact that it can be challenging for model developers and other actors upstream to know when a user intends to create content that is harmful, such measures may be less effective when applied to open-source models and they are not always robust.

Embedding

Embedding involves marking content or attaching information about its origin to indicate whether it is synthetic, and it includes labelling, watermarking and the application of provenance metadata. These techniques are more likely to be effective against deepfakes that defraud and disinform than those that demean.

However, the limitations with embedding techniques are as follows: they will not be implemented by every model developer or deployer; bad actors will attempt to remove embedded information; embedding techniques may be less effective for addressing deepfakes that demean; watermarks can be unintentionally weakened

⁹ C. McGlynn, K. Johnson, E. Rackley, N. Henry, N. Gavey, A. Flynn and A. Powell, "It's Torture for the Soul: The Harms of Image-Based Sexual Abuse" (2021) 30(4) *Social & Legal Studies* 541–562, <https://journals.sagepub.com/doi/full/10.1177/0964663920947791>.

¹⁰ "Martin Lewis felt 'sick' seeing deepfake scam ad on Facebook" BBC News, 7 July 2023, <https://www.bbc.com/uk/news/uk-66130785>.

¹¹ "China, North Korea pursue new targets while honing cyber capabilities" (Microsoft, 7 September 2023), <https://blogs.microsoft.com/on-the-issues/2023/09/07/digital-threats-cyberattacks-east-asia-china-north-korea/>.

¹² D. Siegel and B. Chandra, "Deepfake Doomsday: The Role of Artificial Intelligence in Amplifying Apocalyptic Islamist Propaganda" (GNET, 29 August 2023), <https://gnet-research.org/2023/08/29/deepfake-doomsday-the-role-of-artificial-intelligence-in-amplifying-apocalyptic-islamist-propaganda/>.

through editing; embedding initiatives require close coordination between stakeholders; popularising embedding techniques could result in genuine content being called into question; and more research is needed to understand whether labelling helps users to critically respond to deepfakes.

Detection

Detection refers to techniques that can be used to identify deepfakes and can include the use of forensics, hash matching and user reporting. Such methods are predominantly deployed by online platforms that host content.

The limitation with the detection method, however, is that it faces the following hurdles: bad actors will always seek to adjust their methods to outmanoeuvre forensic techniques; identifying deepfakes requires more than just knowing whether content is synthetic; content editing can diminish the accuracy of deepfake detection tools; hashing techniques can be vulnerable to “collision”; and users of online platforms can find it challenging to identify deepfake content.

Enforcement

Enforcement involves setting and communicating clear rules about the types of synthetic content that can be created using GenAI models and related tools, as well as about the types of content that can be shared on online platforms. It is often the foundation on which platforms build their safety measures, including their approach to moderating content and usage. Enforcement action taken when rules are breached includes issuing warnings to users, taking down content, suspending or removing users and labelling content where there is not a clear breach.

However, although clear terms of service, community guidelines and licence agreements can reduce the ability of bad actors to exploit loopholes whilst also enabling content moderators to make fairer and more informed decisions as they review content, the downside is that polices can suffer from arbitrary boundaries, they can lack specificity and licence agreements are difficult to enforce in the case of open-source models.

Comment

The harmful and often devastating impact of deepfakes continues to be evident worldwide, with California lawmakers approving proposals aimed to protect workers from exploitation by regulating the artificial intelligence industry and combatting deepfakes.¹³ Recently Taylor Swift reportedly felt the need to publicly endorse

Kamala Harris for president as a result of the misinformation shared after Donald Trump posted deepfakes of her falsely claiming to support his candidacy.¹⁴

As AI continues to evolve it will become increasingly necessary for all players in the technology supply chain to take action in order to effectively mitigate the creation and sharing of deepfakes. Such action will need to incorporate a combination of the above strategies and interventions, and if regulated services—such as social media platforms, video sharing sites or search engines—fail to meet their duties under the OSA Ofcom will take enforcement action where needed, including issuing fines and implementing business disruption measures.

While the OSA mainly applies to “downstream” platforms that interface with users, firms that sit further “upstream” in technology supply chains are urged to take equivalent action to address deepfakes. This means committing to some basic, first-principle practices, such as evaluating their models, delaying their release if risks have not been sufficiently mitigated (or gating or removing them in the case of model hosts), and taking appropriate action to block, suspend or otherwise sanction users who breach their rules.

Ofcom is responsible for ensuring that services have the tools they need in order to understand their duties and execute them effectively. As a result, it has also consulted on measures included in its draft Codes of Practice for illegal harms¹⁵ and the protection of children¹⁶ that would help services tackle illegal and harmful deepfakes.

Over the next year Ofcom will examine the merits and limitations of the measures discussed in the discussion paper in more detail, and it may consider including one or more of the measures in a future Code of Practice or guidance. In particular, Ofcom will: (i) examine the role of deepfakes in facilitating fraud offences, which will inform its forthcoming Fraudulent Advertising Code; (ii) explore measures that can address synthetic child sexual abuse material (CSAM), some of which could fall under its definition of a deepfake; (iii) examine the role of deepfakes in facilitating online gender-based violence and abuse, which will inform its forthcoming guidance for services on protecting women and girls; (iv) publish the findings of its research into red teaming; and (v) continue to engage with UK users to monitor how they experience deepfakes online and their wider use and attitudes towards GenAI, as well as continue to support media literacy research and initiatives.

¹³ ABC News, 1 September 2024, <https://abcnews.go.com/US/wireStory/california-lawmakers-approve-legislation-ban-deepfakes-protect-workers-113306224>.

¹⁴ A. Rosenbloom, “Taylor Swift endorses Kamala Harris for president” CNN, 11 September 2024, <https://edition.cnn.com/2024/09/11/0/entertainment/taylor-swift-endorsement-kamala-harris/index.html>.

¹⁵ Consultation: Protecting people from illegal harms online (Ofcom, update 6 March 2024), <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/protecting-people-from-illegal-content-online/>.

¹⁶ Consultation: Protecting children from harms online (Ofcom, update 17 July 2024), <https://www.ofcom.org.uk/online-safety/protecting-children/protecting-children-from-harms-online/>.

In addition, Ofcom will continue to liaise with the Government to identify potential regulatory gaps in relation to deepfakes and GenAI. While the new Labour Government has committed to banning “the creation of sexually explicit deepfakes” the question now arises as to how far Ofcom and the legislature are prepared to row “upstream” with regulation and codes of practice applying directly to developers to control the capacity

of content-creation tools to generate deepfakes that “demean, defraud and disinform”. The UK could be minded to follow (less reluctantly under Labour) the EU’s approach under the AI Act¹⁷ by requiring deployers of AI systems that generate deepfakes to disclose that the content has been artificially generated or manipulated, followed potentially by further guidance on the labelling of deepfakes.

¹⁷ Regulation 2024/1689 laying down harmonised rules on artificial intelligence [2024] OJ L2024/1689.

Publishers of:

European Intellectual Property Review
Entertainment and Media Law Reports
Fleet Street Reports
European Trade Mark Reports
European Copyright and Design Reports

This title is also available as an eBook on
ProView

Visit <https://info.proview.thomsonreuters.com/en.html>
to find out more.



www.carbonbalancedprint.com
CBP2250

**WORLD
LAND
TRUST™**



* 43244692 *