AI CONTENT: THE CHALLENGE OF THE DEEP FAKE

Lorna Skinner KC

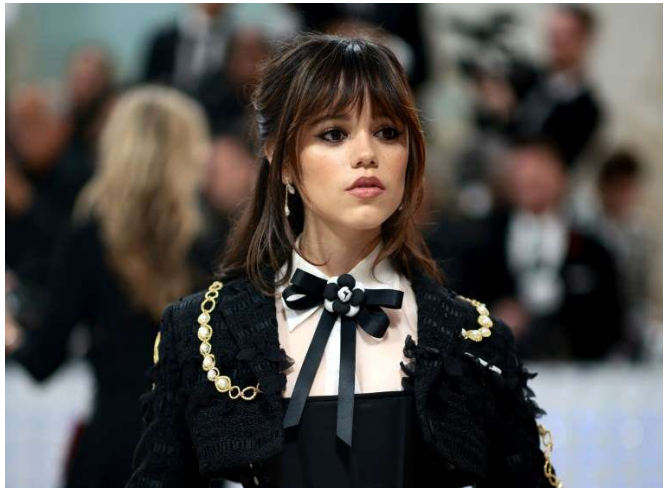
matrix@matrixlaw.co.uk +44 (0)20 7404 3447

matrix chambers

Stephen Fry 'shocked' to discover AI stole his voice from 'harry potter' audiobooks and replicated it without consent, says his agents 'went ballistic'

Bryan Cranston Tells Bob Iger 'Our Jobs Will Not Be Taken Away' by AI in Rousing Speech: You Will Not 'Take Away Our Dignity'

Ads on Instagram and Facebook for a deepfake app undressed a picture of 16-year-old Jenna Ortega



Deep Fake Neighbour Wars

Deep Fake Neighbour Wars uses the very latest in AI technology to turn the UK's best new impressionists into the world's most famous celebrities - only here they are ordinary people who happen to be embroiled in petty silly neighbour disputes

matrix@matrixlaw.co.uk +44 (0)20 7404 3447

matrix chambers

UK's enemies could use AI deepfakes to try to rig election, says James Cleverly

Home secretary, who is due to meet US tech bosses, says states such as Russia and Iran could target other countries as well

Deepfake democracy: Behind the AI trickery shaping India's 2024 election

Want an opponent to campaign for you? Confuse voters between a real and a fake video? As India prepares for the world's largest elections, parties are turning to AI for novel – and dangerous – strategies

The truth behind Trump and his smiling black supporters – they're fake

AI-generated deepfake images of the former president are 'being deployed to influence the outcome of 2024 election', campaigners believe

matrix@matrixlaw.co.uk +44 (0)20 7404 3447

matrix chambers

Deepfake video scams prompt police warning

Fraud makes use of AI technology to steal $25.5 million from HK company

Police are warning businesses and individuals about the growing threat of "AI deepfake" scams after a case in Hong Kong in which a company was deceived out of HK$200 million ($25.5 million) through the use of video conferencing technology.

In the elaborate scheme, a financial employee at the Hong Kong branch of a multinational company received a message purporting to be from the company's chief financial officer in the United Kingdom. The message invited him to participate in a confidential video conference to discuss a transaction.

During the multi-person video call, he interacted with individuals who appeared to be the company's senior executives. However, the participants were actually deepfakes, created using artificial intelligence to superimpose the faces of real people onto fraudulent video footage.

Believing the video call to be legitimate, the victim transferred HK$200 million to designated bank accounts in 15 installments, as instructed by the deepfakes. It was only days later, upon contacting the company's headquarters, that he realized it had been targeted by a sophisticated scam.

In the courts…

Thaler v Comptroller General of Patents Trade Marks and Designs [2021] EWCA Civ 1374

Applicant applied for a patent for an invention generated by artificial intelligence. Application dismissed because under the Patents Act 1977 an inventor must be a person not a machine. Appeal dismissed – no rule of law that the property in a patent generated by a machine was owned by the owner of the machine.

Getty Images (US) Inc v Stability AI Ltd [2023] EWHC 3090 (Ch) – Mrs Justice Joanna Smith 1 December 2023

Declined to strike out proceedings for copyright infringement, database right infringement, trade mark infringement and passing off brought against an open-source generative AI company using a deep learning model to "scrape" millions of images on Getty Images Websites to generate synthetic image outputs in response to commands entered by users.

Harber v Revenue and Customs Commissioners [2023] UKFTT 1007 – 4 December 2023

Cases relied on by a taxpayer in her appeal against a penalty for failure to notify liability to capital gains tax were found to have been generated by an ***artificial intelligence*** system such as ChatGPT. The FTT highlighted the type of harm that was caused by providing fictitious cases, such as causing the FTT and HMRC to waste time and public money, and promoting cynicism about judicial precedents.

Q. 1: “In data protection and privacy cases, how do you control and overcome the legal and practical challenges of deep fakes created by AI?”

Controlling and overcoming the legal and practical challenges of deep fakes created by AI in data protection and privacy cases requires a multi-faceted approach:

1. **Legislation and Regulation**: Enact and enforce laws specifically addressing deep fakes, including penalties for their creation and dissemination.

2. **Technological Solutions:** Develop and deploy advanced AI algorithms and tools for detecting deep fakes, such as digital watermarking or blockchain verification.

3. **Education and Awareness**: Educate the public about the existence and potential dangers of deep fakes, empowering individuals to recognize and report them.

4. **Collaboration**: Foster collaboration between governments, tech companies, researchers, and legal experts to develop comprehensive strategies for combating deep fakes.

Q. 1: “In data protection and privacy cases, how do you control and overcome the legal and practical challenges of deep fakes created by AI?”

5. **Forensic Analysis**: Employ forensic techniques to analyze digital evidence and determine the authenticity of media content in legal proceedings.

6. **Ethical Guidelines**: Establish ethical guidelines for AI researchers and developers to discourage the creation and dissemination of malicious deep fakes.

7. **International Cooperation**: Coordinate efforts on a global scale to address the transnational nature of deep fake threats and ensure consistent enforcement across jurisdictions.

8. **Adaptability:** Continuously monitor and adapt strategies to keep pace with advancements in AI technology and the evolving nature of deep fake threats.

Q.2: “In data protection and privacy cases how do you give clients an edge in legal disputes?”

In data protection and privacy cases, providing clients with an edge in legal disputes involves several key strategies:

1. **Expertise**: Offer specialized knowledge and expertise in data protection and privacy laws, enabling clients to navigate complex legal frameworks effectively.

2. **Risk Assessment**: Conduct thorough risk assessments to identify potential liabilities and develop proactive strategies to mitigate risks.

3. **Compliance Guidance**: Provide guidance on compliance with relevant regulations and standards, ensuring that clients adhere to best practices and avoid regulatory violations.

4. **Evidence Collection**: Assist clients in gathering and preserving evidence, including digital forensics and data analysis, to support their legal claims or defenses.

matrix@matrixlaw.co.uk +44 (0)20 7404 3447

Q.2: “In data protection and privacy cases how do you give clients an edge in legal disputes?”

5. **Strategic Planning**: Develop tailored legal strategies to achieve clients' objectives, whether through negotiation, mediation, or litigation, while considering the unique circumstances of each case.

6. **Preventive Measures**: Implement preventive measures, such as drafting comprehensive privacy policies and implementing robust security protocols, to minimize the likelihood of future disputes.

7. **Crisis Management**: Offer support in managing data breaches or other privacy incidents, including rapid response protocols and communication strategies to mitigate reputational damage.

8. **Advocacy**: Advocate on behalf of clients in legal proceedings, leveraging persuasive arguments and evidence to secure favorable outcomes.

By employing these strategies, legal professionals can provide clients with a competitive edge in data protection and privacy disputes, helping them navigate legal challenges effectively and protect their interests.

matrix@matrixlaw.co.uk +44 (0)20 7404 3447

“Deepfakes” - Some Legal Options

1. Defamation
2. Malicious Falsehood
3. Misuse of Private Information
4. Harassment
5. Data Protection
6. Intellectual Property
7. Criminal Law

matrix@matrixlaw.co.uk +44 (0)20 7404 3447

matrix chambers

“Deepfakes” - Some Legal Options

1. **Defamation**
- False imputation
- Defamatory
- Serious harm

2. **Malicious Falsehood**
- Does not need to be defamatory
- No serious harm threshold
- No single meaning rule

3. **Misuse of Private Information**
- Includes false information
- May well cover intrusive but admitted/obvious deepfakes

4. **Harassment**
- Content does not need to be false
- Requires a course or threatened course of conduct
- Must cross ‘oppressive and unreasonable’ criminal threshold

matrix@matrixlaw.co.uk +44 (0)20 7404 3447

matrix chambers

5. Data Protection

- Processing of personal data - balancing exercise Art 6(1)(f)
- Special category data is not – must fall within Art 9(2)
- Exemptions

matrix@matrixlaw.co.uk +44 (0)20 7404 3447

matrix chambers

Art 9(1) Special Category Data

“ data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation”

Art 4(14) biometric data

"personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data"

Recital 51

The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person

Art 9(2)(e) manifestly made public by the data subject?

ABC v Palmer [2022] EWHC at [76] applying

NT1 v Google LLC [2019] QB 34

ICO Guidance – assumes a deliberate act by the individual

EDPB Guidelines 05/22 – photograph made public does not entail biometric data retrieved by specific technical means is considered as manifestly made public

Public interest special purposes exemption: DPA 1018 Sch 2 Pt 5 para 26

Journalism

Academic

ARTISTIC

Literary

matrix@matrixlaw.co.uk +44 (0)20 7404 3447

matrix chambers

Subject to reasonable belief in:

- public interest and
- that application of the relevant provision of the UK GDPR is incompatible with the special purpose

6. Intellectual Property: Copyright

- Moral rights do not provide any relevant protection
- s30A CPDA 1988 defence of fair dealing with a work for the purposes of caricature parody or pastiche

matrix@matrixlaw.co.uk +44 (0)20 7404 3447

6. Intellectual Property: Passing Off

- Misrepresentation or confusion
- Caselaw includes false representation of product endorsement:
- *Irvine v Talksport Ltd* [2003] EWCA Civ 423; [2003] 1 WLR 1576
- *Fenty v Arcadia Group Brands Ltd* [2015] EWCA Civ 3; [2015] 1 WLR 3291

6. Intellectual Property: Passing Off

Sim v HJ Heinz Co Ltd [1959] 1 WLR 313 at 317; [1959] RPC 75

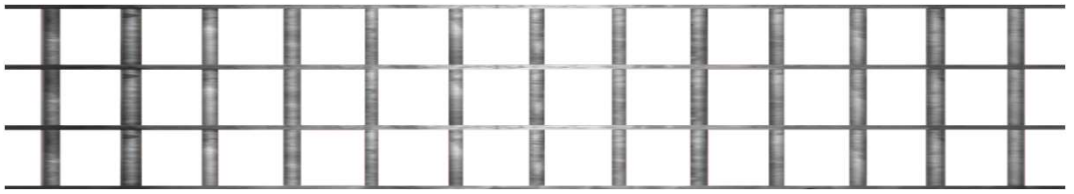
MacNair J "*it would…be a grave defect in the law if it were possible for a party, for the purpose of commercial gain, to make use of the voice of another party without his consent*"

In the Court of Appeal…

Hodson LJ - may be an "arguable case" for passing off, on the basis that the claimant's "*voice as an actor is part of his stock-in-trade and therefore is something which he is entitled to protect as part of his goods*" (at p314 and p319)

Amongst the "*various issues to be determined*", was the question of "*whether this voice can in truth be regarded as a property*" (at p 319)

7. Criminal Law



1. Protection from Harassment Act 1997
2. Various re images of child sexual abuse
3. Communications Act 2003 s127 menacing offensive communications
4. Online Safety Act s179 false communications
5. OSA s181 threatening communications
6. s66A SOA 2003 (amended by OSA) sending images of genitals
7. s66B SOA 2003 (amended by OSA) sharing or threatening to share intimate images

Unlikely to be actionable if…

- Clear and obvious throughout that:
  - the subject has been deepfaked
  - the content is entirely fictional
  - it has been made without the consent of the subject
- Does not feature the subject in any inherently private, distressing or sexual circumstance
- Does not purport to show the subject naked or partially naked
- There is a public interest justification

Thank you for listening.

LORNA SKINNER KC

lornaskinner@matrixlaw.co.uk
Griffin Building, Gray's Inn
London WC1R 5LN
DX400 Chancery Lane, London