How Law Firms Can Protect Their Clients From Deepfakes

Deepfakes are no longer just a concern for celebrities. Synthetic content targeting public figures, influencers, and senior executives is increasingly used to damage reputations, confuse audiences, and put careers at risk. As AI technology becomes more accessible, fraudsters can create convincing fake videos and audio in minutes.

While legislation scrambles to catch up, law firms must take a proactive approach. An AI-driven, legally informed strategy allows firms to monitor, detect, and remove deepfakes at speed and scale before the viral nature of the internet causes irreparable harm.

Step 1: Navigate the Regulatory Framework

Enforcement relies on a cross-jurisdictional approach involving specific AI and data protection frameworks:

- UK Statutory Protections: The Online Safety Act and Data (Use and Access) legislation provide the basis for criminalising non-consensual deepfakes. Ofcom Guidance | Legislation.gov.uk
- EU AI Act & DSA: The EU AI Act mandates transparency and labelling for synthetic content, while the Digital Services Act (DSA) compels platforms to provide priority "Trusted Flagger" status for rapid content removal. EU AI Office
- US Federal & State Laws: The DEFIANCE Act and NO FAKES Act frameworks offer civil causes of action for "digital replicas" and unauthorised likeness use. Congress.gov | FTC AI Strategy
- Regulatory Oversight: Peak bodies like The Law Society (UK), American Bar Association (US), and CCBE (EU) provide essential ethical and evidentiary guidance. Law Society |

Step 2: Implement Proactive Monitoring

Law firms should advise clients to move beyond reactive measures. Prevention starts with detection:

- AI Monitoring: Use specialised software to scan social media, video platforms, and the "open web" for unauthorised likenesses.
- Keyword & Image Tracking: Monitor for specific names, brand assets, and face-match signatures.
- Speed is Critical: Deepfakes spread via viral algorithms; detecting a fake within the first hour can prevent it from reaching millions.

Step 3: Document and Verify the Infringement

To build a strong case for removal or legal action, you must have "airtight" evidence:

- Identify the Source: Track the URL and the original poster (if possible).
- Technical Forensics: Use detection tools to confirm the content is synthetic/AI-generated.
- Preserve Evidence: Take high-quality screenshots and metadata logs before the content is potentially deleted or moved.

Step 4: Provide Proof of Ownership

Since the law takes time to react, "Terms of Service" (ToS) enforcement is often the fastest path to protection:

- Platform Reporting: Report the content directly to platforms (Meta, X, TikTok) for violating impersonation or misinformation policies.
- Cease and Desist: Send formal notices to hosting providers and domain registrars.
- Expert Support: Partner with brand protection specialists who have direct "trusted reporter" status with major platforms to accelerate the removal process.

What Happens Next?

As AI continues to evolve, law firms must remain vigilant. Protecting a client's digital identity requires a blend of legal expertise and technological vigilance. By documenting threats and acting quickly, firms can mitigate the "shock and violation" of a deepfake attack and safeguard their clients' long-term reputations.

Contact Us

Every deepfake or unauthorised digital replica poses a direct threat to your client's professional integrity and commercial value. In an era where synthetic content can spread in seconds, protecting a client's identity isn't just a legal precaution; it's a reputational necessity.

SnapDragon combines AI-powered detection, expert enforcement, and global experience to keep counterfeits off the market and your genuine products where they belong – in customers' hands.

Talk to SnapDragon about how proactive brand protection can drive stronger, more sustainable growth.

www.snapdragon-ip.com

UK & RoW: +44 131 466 9249
US: +1 857 400 7041

thelair@snapdragon-ip.com

LinkedIn

SnapDragon