KOBRE & KIM | DISPUTES AND INVESTIGATIONS

Kobre & Kim's International Private Client Team

Carolina Leung
São Paulo
carolina.leung@kobrekim.com

Emily Beirne
Dubai
emily.beirne@kobrekim.com

Helena Shipman
London
helena.shipman@kobrekim.com

Jacob Kirkham
Delaware
jacob.kirkham@kobrekim.com

Michael Keilty
New York
michael.keilty@kobrekim.com

Polly Wilkins
London
polly.wilkins@kobrekim.co.uk

APRIL 3, 2025

How AI Increases Disinformation Risks for Ultra-High-Net-Worth Individuals

Emerging technologies are creating new reputational risks for ultra-high-net-worth individuals. As bad actors' technological capabilities rapidly evolve and fraudulent activities become increasingly sophisticated, the right tools can aid in mitigating risks and combating harmful online narratives.

This summarizes a Kobre & Kim article coauthored by Polly Wilkins and Helena Shipman for Chambers Global Practice Guides. Click here to read the full article.

Emerging technologies are creating new and evolving reputational risks for ultra-high-net-worth individuals (UHNWIs), presenting new challenges for reputation lawyers, courts, and governments worldwide as they adapt existing tools and introduce new legislation to cover uncharted territories.

As bad actors' technological capabilities rapidly evolve, the potential for damage grows, with spaces once considered safe now causing significant harm. Today, the internet knows no borders, and weaponizing disinformation has become easier, especially through the following tactics:

- **Scraping Personal Information**: AI systems can scrape and republish personal data from online sources without consent. This raises concerns about potential data breaches and the malicious use of personal and sensitive information.
- **Amplification Through Low-Quality Media Sources**: Disinformation can manifest as paid content placed on seemingly credible platforms by third parties. This content is treated as a reliable primary source, leading to further negative coverage in more reputable national or international media outlets.
- **Audio or Video Manipulation**: Deepfakes utilize AI to manipulate video or audio content, altering someone’s face or body with increasingly sophisticated and convincing results. Malicious actors can also use AI to influence search engine optimization (SEO), causing negative content to appear more prominently in search results.

As fraudulent activities become increasingly sophisticated, the risks continue to escalate. Addressing such disinformation can be complex, but the tools listed below can aid in mitigating risks and combating harmful online narratives:

1. **Be Vigilant**. Managing disinformation risks effectively requires a well-prepared team working closely with legal and communications professionals—especially in cross-border disputes, where local expertise is essential to navigating jurisdiction-specific tools and strategies. Monitoring new content as it appears in the public domain and establishing clear escalation protocols and communication channels will enable you to respond swiftly to global developments. Preventing the spread of new factual inaccuracies is just as critical as containing those already causing harm.
2. **Undercut False Statements.** Have an account of the true position ready to deploy and back up critical claims with documentary evidence to the extent possible. Be prepared to respond to and dismantle any false allegations.
3. **Identify Falsehoods and Contact Stakeholders to Correct the Record.** As Google integrates its generative AI system into its search engine, those seeking information about individuals or businesses are potentially presented with inaccurate and/or defamatory information that has been generated from inaccurate data sources. As well as targeting the originating publication, social media platforms, and search engines, consider which stakeholders must be engaged. Ensure that you know who to contact and how to contact them quickly so that you can correct the false narrative and mitigate the harm. As disinformation gains steam, understanding the source and intent behind inaccurate claims is vital to quickly and strategically correct the record and slow down the campaign.
4. **Think Ahead**. Each of the newly available generative AI tools relies on vast amounts of human-generated personal data, making it essential to consider how your current actions may impact future decisions. By anticipating potential scenarios and carefully managing the information you share, you and your team can confidently navigate ongoing disputes.

As emerging technologies enable the spread of false information, at-risk individuals and businesses should take proactive measures to protect themselves from its potentially devastating impact.

About Kobre & Kim

Kobre & Kim focuses on cross-border disputes and investigations, often involving allegations of fraud and misconduct. With 15 cross-border locations, we provide offensive and defensive multi-jurisdiction litigation and crisis management strategies to UHNWIs with global business interests to preserve their assets, liberty, and reputation.

- Our global team includes roughly a dozen former U.S. and UK government lawyers who, along with our civil litigators, sit across EMEA, Latin America, Asia, and the U.S.
- Our industry-recognized experience in helping “businesses and successful individuals to understand and deal with the reputational and privacy issues that have the potential to put them in the spotlight,” according to *Citywealth*.
- Our onshore and offshore lawyers – including an integrated group of U.S. litigators, offshore lawyers qualified in key jurisdictions, Hong Kong solicitors, and English barristers and solicitors – help clients identify vulnerable assets and mitigate reputational harm caused by investigations.
- Our ability to coordinate legal strategy and work closely with various stakeholders (including crisis communications and public relations firms) allows us to formulate holistic strategies to preserve reputation and mitigate privacy concerns.