DEACONS
的近律師行

Deacons Bitesize IP

Intellectual Property

10 September 2024

Shaking off deepfakes?

Ian Liu

Did you know?

The recent posting on Donald Trump's Truth Social platform, of AI-generated images of Taylor Swift falsely suggesting that she had endorsed him, is a timely reminder of the potential and dangers of AI. The Taylor Swift posts are amongst the latest examples of fake endorsements and election-related misinformation in the past year. In the United Kingdom, over 100 deepfake video advertisements impersonating then Prime minister Rishi Sunak were found on Meta's platform, ahead of the United Kingdom general election. In February this year, an AI-generated audio message mimicking the voice of Joe Biden, was used to urge Democratic voters not to vote in New Hampshire's primary election.

Why does this matter to you?

"Deepfakes" are highly realistic video, audio or images generated using AI. Deepfake technology can have many beneficial uses, including simulating surgeries in medicine, creating more interactive teaching materials in education, and developing AI tutors who can provide customised support to students. However, deepfakes can also be used to spread false information, manipulate public opinion, or by scammers. A multinational company in Hong Kong recently lost HK$200 million (US$25.6 million) in a scam after employees were fooled by deepfake technology including a video conference call where a digitally recreated version of the company's chief financial officer ordered money transfers to be made.

The World Economic Forum has ranked disinformation as a top global risk for 2024, with deepfakes as one of the most worrying uses of AI. As the law struggles to keep up with the developments in AI technology, major jurisdictions are attempting to implement solutions to protect against the misuse of a person's name, voice, image and likeness.

In the US, there is currently a patchwork of state and local laws attempting to govern AI technology including Taylor's Swift's home state of Tennessee, which recently enacted the Ensuring Likeness Voice and Image Security Act or "ELVIS Act", aimed at protecting people from unauthorized use of content that mimics their voice or image. The US is drafting new federal laws to protect against harmful deepfake content including the Content Origin Protection and Integrity from Edited and Deepfaked Media Act, introduced into the Senate in July.

In Europe, the AI Act is now in force, imposing strict transparency requirements on the providers and users of AI systems, so that systems creating deepfakes must mark their output as artificially generated or manipulated, and users must disclose whether AI has been used to create or alter content.

China's Deep Synthesis Provisions introduced in January 2023, prohibits the use of deepfake technology for spreading "fake" news or information that could disrupt the economy or national security. Amongst other obligations, providers of "deep synthesis technologies" are also required to take steps to prevent the use of their services for illegal or harmful purposes, and must label synthetic content.

In Hong Kong, the recent public consultation paper on "Copyright and Artificial Intelligence" acknowledges that deepfakes and the transparency of AI systems are important topical issues that are closely related to various other domains. However, it would not be appropriate to address them separately and solely from the perspective of copyright.

Hong Kong does not have a freestanding right of personality or publicity. However, the Government believes that unauthorised use or imitation of a person's name, likeness, voice, or other indicia of identity by means of deepfake technology, is already actionable under the existing legal regime. For instance, when the deepfake content involves unauthorised use of a copyright work, trade mark and/or making of a misrepresentation causing damage to one's goodwill, legal action may be brought on the basis of copyright infringement, trade mark infringement and/or the common law tort of passing off, depending on the circumstances. Certain non-IP laws governing matters such as personal data protection, defamation, the publication of unauthorised intimate images, fraud, or deception, may also apply where there has been use of untrue or inappropriate information created by deepfakes.

The paper noted that other jurisdictions are introducing specific measures to regulate the misuse of deepfakes but these are not primarily driven by IP concerns. Meanwhile, the Government has commissioned a local research centre specialising in generative AI to help examine and suggest appropriate rules and guidelines, from the user and industry perspectives, on the accuracy, transparency and information security of generative AI technology and its applications. Watch this space.

Want to know more?

Ian Liu
Partner
ian.liu@deacons.com
+852 2826 5360