withers



ARTICLE

Deepfakes, digital evidence and family disputes: when authenticity becomes an issue

13 OCTOBER 2026 | APPLICABLE LAW: HONG KONG | 3 MINUTE READ

GET IN TOUCH

From WhatsApp messages and emails to photographs, voice notes and video recordings, digital evidence has become a central feature of modern family disputes.

Allegations concerning hidden assets, family violence, parenting arrangements and the conduct of a spouse increasingly turn on electronic records that may appear, at least on their face, to provide an objective account of events.

The emergence of generative artificial intelligence is beginning to challenge that assumption. Advances in AI have made it possible to create highly convincing fabricated content, including altered photographs, cloned voices and realistic videos portraying events that never occurred. At the same time, the proliferation of deepfake technology has created a further complication: parties faced with genuine evidence may seek to dismiss it as artificially generated.

As a result, a new question is beginning to emerge in family disputes: how should parties, lawyers and courts approach digital evidence where authenticity itself is in issue?

An emerging challenge for family proceedings

Family disputes can be particularly vulnerable to concerns over manipulated evidence.

Unlike many commercial disputes, family cases often involve events that occur in private and without independent witnesses. Courts are therefore frequently asked to consider communications between family members, recordings of conversations, photographs and other forms of digital evidence in order to determine what occurred.

Historically, the authenticity of such material was often assumed unless there was a specific reason to challenge it. AI-generated content is beginning to change that landscape.

The issue extends beyond entirely fabricated material. Content may be selectively edited, taken out of context or enhanced in ways that alter its apparent meaning. Equally, the increased public awareness of deepfakes may encourage parties to challenge legitimate evidence simply because technological manipulation is now possible.

The result is that courts may increasingly need to examine not only what a piece of evidence appears to show, but also where it came from, how it was created and whether its integrity can be independently verified.

How are courts responding?

Although reported cases involving AI-generated evidence in family proceedings remain relatively limited, courts are already grappling with the implications of generative AI.

In Singapore, the judiciary has issued formal guidance governing the use of generative AI in court proceedings, including matters before the Family Justice Courts. The guidance emphasises that parties remain responsible for ensuring that material presented to the court is accurate and independently verified.

Recent Singapore family proceedings have also highlighted the risks associated with overreliance on AI-generated content. Courts have encountered instances where litigants relied on authorities generated by AI which proved to be entirely fictitious, reinforcing the principle that responsibility for the accuracy of court materials ultimately remains with the party submitting them.

In Hong Kong, established evidential principles continue to provide the framework for assessing disputed digital evidence. The Hong Kong Judiciary issued guidelines in July 2024 highlighting the risks associated with the use of artificial intelligence and cautioning judges and court users about issues relating to authenticity, reliability and evidential weight. As AI-generated content becomes increasingly sophisticated, these considerations are likely to assume even greater significance.

Users must remain mindful of both the capabilities and limitations of the generative AI tools they use. Any information generated through such tools should be carefully reviewed, verified and validated to ensure its accuracy and reliability before it is used or relied upon in the course of their work.

These concerns form part of a broader evidential challenge: evidence may be manipulated not only through technology, but also through pressure placed on a witness. In HKSAR v LCL [2023] HKCA 1301, the Court of Appeal considered a scheme in which family members influenced a minor witness to change her account and caused her and another prosecution witness to leave Hong Kong. Although the case did not involve deepfakes or AI-generated material, it illustrates the serious consequences of attempts to distort the evidential record and the importance of testing evidence against its provenance, surrounding circumstances and independent corroboration.

Testing authenticity through digital forensics

Where authenticity is challenged, technical analysis may become a critical part of the evidential picture.

Determining whether a document, image, audio recording or video has been manipulated is rarely as straightforward as identifying a single "tell-tale" sign. Modern AI tools can produce highly convincing material,

while legitimate files may exhibit anomalies as a result of compression, conversion or routine editing processes.

Forensic analysis often involves examining the broader digital footprint surrounding a piece of evidence. In practice, digital forensic investigations rarely begin with the assumption that a document or image is either genuine or fabricated. Instead, specialists seek to establish the integrity and history of the evidence before drawing conclusions. Forensic analysis often starts with understanding the origin of the material. Experts may ask how a file was obtained, as establishing the chain of origin is critical when assessing authenticity.

Digital forensic specialists also examine metadata, often described as the 'digital fingerprint' of a file. Metadata can provide valuable information regarding when a document was created, modified, transferred or accessed and may determine the chain of custody. Video and audio recordings often require multiple levels of analysis. Beyond reviewing visual content, experts may examine embedded metadata, editing histories, compression patterns and audio waveforms. Where only scans or copies of documents are available, comparisons between file metadata, storage device records and contemporaneous documents may assist in determining whether alterations occurred prior to scanning or transmission.

There is no single indicator that confirms a document, photograph, audio recording or video has been generated or altered using modern AI tools. Forensic analysis may focus on the totality of the evidence rather than isolated irregularities. They may include:

- Inconsistencies in lighting, shadows, or reflections
- Unnatural hands, fingers or facial features
- Visual elements that appear excessively uniform or 'too perfect'
- Irregular pixel patterns that become apparent when images are examined at high magnification
- Metadata that is inconsistent with the origin of the file

Importantly, the objective is not simply to determine whether a particular file was generated using AI. In many cases, the more significant question is whether sufficient confidence can be placed in the integrity and reliability of the evidence as a whole.

Protecting and preserving digital evidence

Parties who suspect that digital evidence may be disputed should consider taking steps to preserve the original material as early as possible.

Original files are often more valuable than screenshots or forwarded copies, and the surrounding context of a communication may be just as important as the communication itself.

Early advice can also be critical. By the time authenticity becomes a contested issue in litigation, valuable information may already have been lost through device changes, deleted accounts or routine system activity.

The quality of a forensic examination is often determined by the quality of the evidence preserved at the outset. For this reason, parties should consider preserving original material as early as possible.

Where authenticity is likely to become an issue:

- Consult with your solicitor as soon as possible, and let the solicitor guide you through the process
- If the evidence is crucial to the case, preserve the original device on which the evidence was recorded and, if possible, avoid using the device further
- Write down exactly how this file came into your possession so the information is kept accurate
- Where documents must be digitized, high-resolution scanning (at 600 dpi) is generally preferable to photographing them

The future of digital evidence

The increasing accessibility of AI-generated content is unlikely to diminish the importance of digital evidence in family disputes. If anything, it is likely to make questions of authenticity more significant.

For family lawyers, the challenge will be balancing a healthy degree of scepticism with an appreciation that most digital evidence remains genuine. For clients, the key issue may no longer be whether a document, image or recording appears convincing, but whether its provenance and integrity can ultimately be demonstrated.

As technology continues to evolve, collaboration between legal advisers and forensic specialists is likely to play an increasingly important role in helping courts distinguish between authentic evidence and digital fabrication. Practitioners should avoid assuming that everything is either real or fake. The most effective investigations begin with an open mind and a willingness to test competing explanations before reaching conclusions.

Get in touch



Jocelyn Tsao

PARTNER | HONG KONG

VIEW PROFILE



Anisha Ramanathan

PARTNER | HONG KONG

VIEW PROFILE



GUEST SPEAKER

Anthony Tsang

DIRECTOR | THE FORENSICS COMPANY