

Insights

WHEN DISCLOSURE GOES WRONG: PRACTICAL LESSONS FROM CABO CONCEPTS LTD & ANOR V MGA ENTERTAINMENT (UK) LTD & ANOR

Oct 26, 2026

In *Cabo Concepts Ltd & Anor v MGA Entertainment (UK) Ltd & Anor* [2026] EWHC 768 (Ch), Mrs. Justice Bacon considered circumstances in which both parties had fallen significantly short of their disclosure obligations. The central question was whether those failings, ranging from missed instant message chats to hundreds of thousands of uncollected emails, justified reopening a final costs order. Below, we outline the disclosure issues and the practical lessons they carry for document collection.

In numbers: 84,000 emails from one custodian went uncollected by MGA. By the next hearing, that figure had grown to 800,000 missing documents. A court-ordered re-run later uncovered 7.5 million more. A second attempt at disclosure of mobile data by Cabo turned up a 583-page "Top Secret" messaging app chat that the Court found was the founders' primary means of communication throughout the relevant period.

The background

The underlying claim concerned allegations that MGA stifled the UK launch of Cabo's "WorldeeZ" toy through anticompetitive conduct and unjustified threats of patent infringement. The trial, originally listed for June 2022, was adjourned shortly before it was due to start after serious deficiencies in MGA's disclosure. As a result, in 2022, MGA were ordered to pay indemnity costs and were required to make a payment on account of £578,444.17.

The case eventually proceeded to trial in 2024–25. The Court found that MGA's conduct amounted to an abuse of a dominant position and unjustified threats, but that Cabo would not have traded profitably in any event, so the damages claim failed.

After trial, MGA sought to revisit the 2022 costs order. It relied on disclosure breaches by Cabo that had come to light during the intervening period, in particular, the failure to collect significant volumes of data from a communication platform, as well as inaccuracies in the evidence given by Cabo's solicitor at the original hearing. MGA asked the Court either to set aside the indemnity costs

order entirely or to substitute a reduced order on the standard basis. The application, heard in January 2026, therefore required the Court to decide whether those later-discovered failings justified varying a final costs order.

Disclosure issues

MGA's disclosure failings

In June and July 2022, MGA informed the Court of the scale of the disclosure issues. The collection exercise had been undertaken by MGA's in-house IT team without oversight from an e-disclosure specialist.

Although the errors were not deliberate, Joanna Smith J found that MGA's conduct fell outside the norm. The Court expressed concern about the scale of the technical failings, MGA's failure to spot clear warning signs, and its continued lack of supervision even during the re-harvesting exercise. A Court-ordered re-run, conducted by an external provider, then uncovered more than 7.5 million previously uncollected documents (significantly more than the estimated 800,000 missing documents). Of these 47,656 were ultimately disclosed, accounting for around 80% of MGA's total disclosure.

Cabo's disclosure failings

Cabo also faced significant disclosure problems. Following queries raised by MGA in April 2023, a re-collection of mobile phone data by Cabo's provider uncovered additional mobile messaging correspondence and more than 4,000 images, including the "Top Secret" chat that the Court later found was the founders' primary means of communication during the relevant period. Further issues emerged in May 2024, with over 1,000 documents identified.

The Court found that Cabo's solicitor had relied largely on informal discussions with a key custodian and had failed to provide clear instructions or adequately supervise the search process.

The Court reiterated that while clients may search their own devices, solicitors must take reasonable steps to advise, assist and supervise those searches. Cabo's solicitor had not enquired into how the searches were carried out and accepted limited material without question. The Court rejected the suggestion that the shortcomings were merely accidental, concluding that the search *"was carried out, from the start, in entirely the wrong way"*. As a result, Cabo's disclosure certificate was found to be materially inaccurate.

Why the costs order remained unchanged

The Court declined to revisit the costs order. Emphasising the importance of finality in costs decisions, Mrs Justice Bacon held that the costs order was based on MGA's own disclosure failings and remained sound notwithstanding Cabo's later-discovered breaches.

The Court observed that revisiting earlier costs decisions with the benefit of hindsight would be "a recipe for chaos" in complex litigation. MGA's application was therefore dismissed. The Court did, however, order Cabo to pay the costs MGA had incurred investigating Cabo's disclosure failings and reviewing the late-disclosed material, an outcome that Cabo had not opposed.

The takeaway

The judgment is a stark reminder that disclosure is only as reliable as the processes underpinning it. The decision underlines the importance of active oversight by legal teams, particularly where searches are carried out by clients/internal IT teams themselves or delegated to third-party providers. At the same time, it reaffirms the Courts' commitment to the finality of costs orders. Even where significant disclosure failures come to light later, parties should not expect the Court to revisit a costs order that was properly made on the information available at the time.

Practical guidance

Technology alone does not ensure disclosure compliance. In practice, successful disclosure exercises are typically underpinned by a combination of technical expertise, effective legal oversight, and defensible workflow processes. The issues encountered by both parties in *Cabo v MGA* serve as a useful reminder of the importance of getting each of these elements right from the outset.

Engage specialists early

Whether through a law firm's dedicated forensic technology team or an external eDisclosure provider, involving specialists at an early stage can significantly reduce risk. A properly scoped data mapping exercise should identify key custodians, data repositories, communication channels, devices, cloud platforms, and collaboration tools from the outset. Particular attention should be paid to less formal messaging and communication platforms which increasingly contain some of the most relevant and contemporaneous evidence in disputes. While there may be circumstances where self-collection is appropriate, there are many situations where specialist expertise is required to address issues such as deleted content, retention and backup settings, application-specific data stores, and data preservation requirements. Custodians remain critical in identifying relevant sources, but independent forensic professionals provide an additional layer of defensibility and assurance. They can also assist in identifying technical risks, validating collection methodologies, ensuring preservation obligations are met, and implementing robust quality control procedures. As demonstrated in this case, mobile and messaging data should not be treated as an afterthought and may, in some instances, represent the primary evidential data source.

Maintain active legal oversight throughout the disclosure process

Disclosure responsibilities **should** not be carried out entirely by clients/their internal IT teams, or entirely delegated to third-party providers. Legal teams should have a clear understanding of the disclosure exercise and be able to explain what was collected, how collections and searches were conducted, why particular sources were included or excluded, and what quality assurance measures were applied. That understanding should be reflected in disclosure certificates and supported by appropriate documentation. A well-prepared and actively managed Disclosure Review Document (DRD) remains one of the most effective tools for ensuring alignment between legal strategy, disclosure obligations, and the underlying technical process.

Prioritise defensibility and auditability at every stage

A collection exercise should not be considered complete simply because data has been exported. Proportionality and reasonableness require ongoing validation throughout the disclosure lifecycle. Effective quality control measures may include verifying mailbox sizes against collected content, conducting sample collections to test completeness, reviewing date ranges for unexplained gaps, comparing collected document volumes against expected data volumes, and investigating anomalies or obvious "red flags" as soon as they arise. The Courts are unsympathetic where warning signs were present but not acted upon.

Equally important is the creation and maintenance of a comprehensive audit trail. Collection, processing, and review decisions should be documented throughout the matter, including who performed the collection, when and how it was undertaken, the systems and devices examined, the search methodologies applied, and any exclusions, limitations, or technical issues encountered. These records can prove invaluable if the disclosure process is later challenged.

Finally, disclosure should not be viewed as a one-off exercise. As matters evolve, new custodians may emerge, issues may develop, and additional sources of potentially relevant information may be identified. Collection strategies should therefore be revisited periodically to ensure they remain appropriate, proportionate, and complete. Regular reassessment is often the best way to identify and address gaps before they develop into costly disclosure disputes.

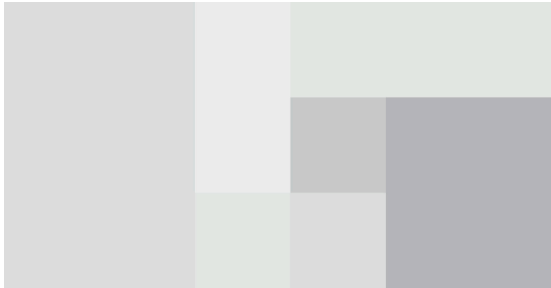
The broader lesson from *Cabo v MGA* is this: defensible disclosure is rarely the product of a single technology, tool, or individual. It is produced, through specialist expertise, active legal supervision, and processes rigorous enough to withstand scrutiny when it matters most.

The authors would like to thank Trainee Solicitor Nadra Ali-Elmi for their contributions to this insight.

Related capabilities

- Business & Commercial Disputes

Meet the team



Samantha Hewitt

Senior Associate, London

sam.hewitt@bclplaw.com

[+44 \(0\) 20 3400 2363](tel:+442034002363)



Jason Alvares

Head of Forensic Services, London

jason.alvares@bclplaw.com

[+44 \(0\) 20 3400 3272](tel:+442034003272)

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.