Deloitte.

Discovery insights

5 questions about global litigation holds

An interview with Michael Weil, managing director,
Deloitte Financial Advisory Services LLP

The intent of a litigation hold is generally clear—the preservation of electronically stored information and documents potentially relevant to a pending legal matter. When a hold actually looms, however, odd things can happen. Custodians may delete files or alter documents in the service of protecting the company, their boss, or themselves. If it's a cross-border matter, some may simply defy the mandate, reasoning that they are compliant with their home country laws and thus are protected from the foreign dictates.

Whatever the motive, failure to abide by a hold can have potential consequences for both the individual and the organization, up to and including obstruction of justice criminal charges with stiff penalties and possible reputational damage.. Exploration of several hold-related questions can help multinational companies understand the vagaries of cross-border discovery and comply with dictates of the jurisdictions in which they operate.

Question #1: What is distinctive about legal hold requirements in cross-border litigation?

Hold policies can vary from country to country in terms of law; practice; and culture, including data privacy requirements. For companies involved in global litigation, these distinctions raise issues for both data custodians and the information technology (IT) organization along with their legal counsel and executive leadership.

An overarching factor is the fundamental differences in the legal systems of various countries. Nations including the United States, Canada, India, and the United Kingdom are governed by "common law" systems, in which case law formed through judicial opinions predominates. Other countries, including China, Japan, and continental Europe nations, adhere to "civil law," which is guided by codified statutes. Under civil law, the concept of e-discovery is fundamentally different from those in common law countries.

For example, a custodian in a German company who is directed to produce evidence for a US proceeding may choose to ignore the dictate, regarding it as American overreach. Because this stance may not run afoul of German law, and Germany does not extradite its citizens to other countries, the custodian may have no fear of consequences from not preserving and producing the information.

In an international investigation, however, the arm of the law is long. Upon traveling to another country, the offending custodian could become subject to a US warrant and be taken into custody.

A cross-border hold can also cause headaches for technologists in the custodian's company. IT department personnel may not understand what they need to preserve, or the risks involved in not doing so, or they may not realize documents are stored in a jurisdiction with differing privacy laws than the jurisdiction the IT staff sits in. Because their job description focuses on keeping systems running and available to the business, data preservation may be an afterthought. A broader view of preservation among both custodians and IT personnel is imperative in the global business environment.

Question #2: How does the ease with which documents can be deleted affect preservation?

Deletion of potentially responsive evidence can be as simple as a keystroke, impossible to undo, and monumentally important to a legal matter. Sending data to the recycle bin or the deleted items folder may be construed as a willful step along the path to getting rid of it. Emptying that repository then furthers the act and may further affirm the actor's intent.

That doesn't mean the data is lost, however, or the steps have gone unnoticed. Systems and forensic investigators are increasingly able to uncover deletion efforts, as well as actions taken to alter files to eliminate or change potentially responsive or incriminating content. Given the diminishing odds of such steps succeeding, potential perpetrators would do well to remember the admonition that, "Sometimes it's not the crime, it's the cover-up."

In some cases, custodians may delete data from systems but save it to an external drive or other external device. Such actions are still traceable, placing the custodian in jeopardy. Because the data still exists, however, an argument can be made against an obstruction of justice charge if the external drive is handed over.

Question #3: How effective are existing methods of data recovery?

Information that has been deleted can continue to exist on a storage medium for some time, commonly until it is overwritten with other data. Nonetheless, evidence degrades over time, and the further from the deletion event, the harder it is to recover with traditional methods, which are simply not that effective.

Stipulating a healthy dose of "it depends," our past experience at Deloitte has been that about 10–20 percent of deleted files can usually be recovered through traditional data recovery methods. Thus, where internal bad actors may have willfully misbehaved, the 80–90 percent of data that is unrecoverable represents an incremental risk exposure to the custodian's company. Whether data loss factors into an obstruction of justice charge or an adverse legal presumption can depend on factors such as whether or not having the data prejudices the investigation to the alleged perpetrator's benefit. Conversely, more data recovered may mean further risk mitigation and potentially reduced consequences to the company. For the alleged perpetrator, in contrast, more data can create greater exposure.

Question #4: What innovations are emerging to increase data recovery and mitigate the risks of custodian misbehavior and mistakes?

Merely thinking about recovery more broadly is one important step. While traditional recovery methods generally produce the 10-20 percent recovery rate noted above, a more expansive, innovative approach could dramatically increase that figure.

Deleted files leave certain markers—names, sizes, dates, and times. If another file is found with the exact same markers, it is likely to be the same as the one that was deleted. In the hands of a capable

forensic investigator, a forensic intelligence platform can support such exploration, as a recent Deloitte assignment illustrates. That investigation focused on uncovering instances of data destruction across 1,000 pieces of media. Using the platform, investigators were able to search for instances of the file markers described above, along with indicators of file sharing, to find an existing, active copy of certain files and recover them. In some instances, our methodology recovered over 85% of the deleted files.

Question #5: Can investigators benefit from tying recovery innovations to document review?

Traditional forensic analysis focuses on how much data can be recovered. Applying the 10-20 percent benchmark noted above, if 10,000 files were deleted, 2,000 or so might be resurrected. Using the techniques described above, along with the advanced forensic intelligence platform, the number could potentially rise into the 8,000 range.

Whatever the number, the question that may be of most interest to a judge is how many files are potentially relevant to the matter at hand. Tying the forensic intelligence process to a document review platform could help determine which of the recovered files—whether 2,000 the old way or 8,000 using the new tools—are responsive or not.

Tying the deletion and recovery efforts to the review process in this manner can help improve the recovery effort and understanding around the data deleted, such as the responsiveness of the deleted data to the matter.

My take

Data custodians around the world can get quite edgy, or in the extreme, defiant, when a foreign jurisdiction dictates that their organization place information under legal hold pursuant to an investigation. The legal, practical, and cultural disparities between countries—notably when the United States is involved—can lead to misunderstandings, false conclusions, and resistance to cooperation. Based on their own experience, their concerns about data privacy, or a sense of panic, custodians can misbehave. When they do, innovative tools and techniques now available can help investigators identify tampered-with data, recover it, and determine its relevance to the matter at hand.

Let's talk:

Michael Weil
Managing Director
Deloitte Financial Advisory Services LLP
+1 312 486 0207
miweil@deloitte.com

Deloitte.