Understanding ESI Chain of Custody

For most people the phrase “chain of custody” conjures images of smoking guns and drug busts, writes Indiana lawyer Helen Geib on **QDiscovery**‘s website. The importance of chain of custody in criminal cases is well known, and police and prosecutors have clear and detailed guidelines for handling physical evidence. By contrast there is relatively little understanding of the unique problems and considerations underlying chain of custody for electronic evidence. However, given ESI’s ubiquity and high risk of (usually inadvertent) spoliation, ESI chain of custody is an issue that civil litigators cannot afford to ignore.

Her article continues:

Defining “Chain of Custody”

The Electronic Discovery Reference Model’s online glossary defines chain of custody as:

“All information on a file’s travels from its original creation version to its final production version. A detailed account of the location of each document/file from the beginning of a project until the end. A sound chain of custody verifies that you have not altered information either in the copying process or during analysis.”

In other words, chain of custody shows a) where the evidence has been; b) who has touched it; and c) its condition at all times. It tracks an object or file through the evidence lifecycle of:

– Collection at the source;
– All transfers between source and courtroom;
– Storage; and,

– Handling for inspection, review, and forensic examination.

The norm is to demonstrate that there has been no change in the condition of the evidence. Where evidence is altered- for example, taking a sample of the white powder to send to the drug lab for analysis- the chain of custody must document the circumstances and details. This is of acute importance in forensic examination of computers, mobile phones, and other electronic devices, as forensics frequently necessitates making some changes to the source media or files. Documenting what happened does not prove that the alteration was necessary and appropriate; that must be independently demonstrated.

How ESI Chain of Custody Is Different

A principal distinction between ESI and physical evidence in the context of chain of custody is that ESI involves copies: an object is picked up and moved; an electronic file is copied. The differences start at the point of collection. In contrast to seizing an evidence item, chain of custody for an electronic file establishes that an identical copy has been created. In fact, ESI may potentially be copied many times over in the course of collection, transfer, and handling.

Another important distinction is that eDiscovery routinely involves altering evidence by changing the file format. Lawyers' continuing preference for TIFF or PDF production format (ideally with linked metadata, extracted text, and for certain data types, native files) makes file format changes both necessary and desirable. The key point here is to show that the information contained in the file has not been altered in the course of ESI processing, review, and production.

Why Chain of Custody Is Important (and its Limits)

Chain of custody is an essential part of authentication. It shows:

– Provenance- This picture was found on the cell phone seized from the suspect on such and such date, or this Excel spreadsheet was copied from the company's server at this folder location; and,
– Integrity- The knife had this person's fingerprints on it when it was picked up at the scene, or this PDF is a true and accurate copy of the text content of the Word document copied from the witness' computer.

What chain of custody does not show is what happened before collection. For instance, it is not in itself evidence that the owner of the computer created the files found on it, and it is similarly silent as to who had access to the computer pre-collection or what programs were installed. And of course, it is not relevant to understanding meaning or significance.

Who is Responsible for Chain of Custody

Primary responsibility for maintaining ESI chain of custody rests with whoever is in possession of it at any given time. Most of the time in civil discovery this is the eDiscovery services provider. Having defensible chain of custody procedures should always be considered in vendor selection.

Responsibility will shift to, or be shared with, the client when IT staff or individual document custodians are involved in data collection. Failure to keep good documentation is one of the most significant risks of unsupervised client self-collection. Finally, post-production, law firms and lawyers must take care not to alter ESI, particularly files produced in native format.