Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Changes to the Federal Rules of Evidence – Rule 26

As of December 1, 2010, the rules have changed. The Federal Rules of Evidence (FRE) provide the basis for expert testimony and the requirements for expert reports and qualifications for all Federal cases, and is reflected in many State and local jurisdictions, typically with some delay. After an extensive processes, supported by the legislative and judicial branches of government, including the Supreme Court, the rules have changed. While these changes may seem relatively simple, for the digital forensic evidence examiner and other expert witnesses, there is quite a substantial difference that will reduce costs, ease burdens, and allow examiners and lawyers to focus more clearly on the things they should be doing with regard to legal matters.

Rule 26 – the duty to disclose

Rule 26, part of the "Federal Rules of Civil Procedure", deals with the "Duty to Disclose; General Provisions Governing Discovery". Discovery is the process by which litigants are able to get the information they need in order to litigate the legal matter. The changes to Rule 26 that effect experts and their work are to subparts 26(a)(2)(B) (Witnesses Who Must Provide a Written Report) and 26(b)(4)(B) and (C) (Discovery Scope and Limits: Trial Preparation: Experts.). In essence, the rule changes force the disclosure of the full basis for claims made by experts and, at the same time, reduce or remove the requirements associated with experts disclosing communications and drafts.

Rule 26(a)(2)(B) – Expert Reports, Opinions, and Their Basis

Rule 26(a)(2)(B) includes, in pertinent parts:

> an expert witness must provide an expert report and "...The report must contain: (I) a complete statement of all opinions the witness will express and the basis and reasons for them; (ii) the facts or data considered by the witness in forming them; (iii) any exhibits that will be used to summarize or support them; (iv) the witness's qualifications, including a list of all publications authored in the previous 10 years; ..."

This rule properly puts the burden for providing the basis for opinions from the side challenging the witness to the side putting forth the witness, in that under the old rules, it was up to the other side to ask for the basis and the facts, and given the time frames for different phases of discovery, this was often problematic.

Perhaps more importantly, this puts the scientific burden for experts where it belongs - on the experts. The courts have long insisted that expert testimony be the result of reliable methods reliably applied, but most expert reports I have reviewed in digital forensics to date failed to provide the vast majority of the key information required in order to evaluate the opinions stated. For example, and without limit, I have seen digital forensics reports stating things like "[strings were] randomly generated" and "[there is] no such person", but the authors provided no basis at all for these rather startling conclusions.

My high expectations anticipate that we will start to see expert reports that state a substantial basis for the opinions offered. For example, I hope they start to (1) identify the method used, (2) provide citations to peer reviewed articles characterizing the methods, (3) identify how the mechanisms they used to implement the methods have been tested and calibrated, (4) provide references to or study information relating to the limits and/or reliability of the methods and mechanisms, and (5) provide a reasonably detailed background on the mechanisms under study and how and why they are reasonably examined using the identified methods. I certainly try to do this in my expert reports and teach students to do this as well.

But there are limits to the extent to which a basis may be or should be provided. At the fringes, there will likely always be (1) reports that state a minimal basis (e.g., based on my many years of work experience in the field) without providing any reliability information (i.e., based only on all that experience, and with no actual studies or scientific evidence, how do we measure your reliability) and (2) lawyers who challenge the level of depth of the basis no matter how detailed it is (e.g., so what is the underlying basis for your claim that bits are the lowest level atomic thing represented in digital form?).

My rule is that you should provide enough basis so that somebody who is familiar with the art in the field and properly skilled, educated, and/or experienced in the art, after reading the specific references cited and the details provided, can (a) understand precisely what is being claimed and why, and (b) independently validate and/or verify any results, given proper resources.

Rule 26(b)(4)(B)and(C) – Discovery Limits

In pertinent parts:

> "(B) Trial-Preparation Protection for Draft Reports or Disclosures. Rule 26(b)(3)(A) and (B) protect drafts of any report or disclosure required under Rule 26(a)(2) regardless of the form in which the draft is recorded. (C) Trial-preparation Protection for Communications Between a Party's Attorney and Expert Witnesses. Rule 26(b)(3)(A) and (B) protect communications between the party's attorney and any expert witness required to provide a report under Rule 26(a)(2)(B), regardless of the form of the communications, except to the extent that the communications: (i) relate to compensation for the expert's study or testimony; (ii) identify facts or data that the party's attorney provided and that the expert considered in forming the opinions to be expressed; or (iii) identify assumptions that the party's attorney provided and that the expert relied on in forming the opinions to be expressed."

In other words, since the report contains the basis for their opinions, including everything they considered or relied upon in forming those opinions, they are not exempt, because they have to be provided per the previous rule change. But everything else, is now confidential. This is a big deal for those who are engaged in this activity, for several reasons.

1. It means that experts and attorney's don't have to go through elaborate means to communicate in such a manner as to not create a record when reviewing reports or discussing alternative approaches. There is nothing illegitimate about an attorney going over a report and discussing what it includes or doesn't include with an expert and asking, for example, for expansion in a particular area, or a better explanation.

2. It saves lawyers and experts having to fly across the country to meet in person so that, for example, an expert can look at potential evidence and help the attorney decide whether it is relevant or not, without potentially exposing it to the other side. A good example is audit trails containing elements of confidential medical records that are not relevant to a legal matter, but that would get exposed unnecessarily unless reviewed by someone who knows the difference between different sorts of audit records that relate or don't relate to matters at issue in the case. Now these records can be communicated to the expert who can work on them in their own facility and then dispose of those that are not relevant.
3. It means that, as an expert, I can write down theories about the case that I may have without having to expose the theories I discarded, for good reason, to the other side. As I explore a case, I have such theories all the time, but up until this time, I had to either keep them in my head, or place them all into the draft report, which I don't retain copies of for other good reasons, and then remove them as I worked through them. Otherwise, the other side might get all sorts of wrong impressions about notions that did not pan out. Similarly, I can act as an expert advising attorneys about issue that I don't end up testifying about while still testifying about other issues in the case and without exposing the other issues to the other side.
4. It means that I don't have to have a separate set of backups and other mechanisms to assure that older versions are no longer retained by accident. While my normal process does not retain drafts because I find it confusing, my backup processes for normal systems are less complicated because I don't have to worry about having to search for residual drafts and similar content that might remain in older backups. I still have to deal with the issues of mandatory destruction of confidential data, and thus my forensics backup system has to be kept properly controlled to a different level than my normal backup system which does not contain such restrictions, but I can use standard commercial methods, enable automated search methods on my systems, and so forth, instead of having to have a completely different approach to forensics-related issues.

To reiterate, none of these things are intended to, nor do they have the effect of, causing any disadvantage to the other side in a case, in terms of my actual opinions in the matter at hand. What they largely avoid is large volumes of meaningless content being redundantly pushed onto larger and larger storage media to support the unnecessary redundancy associated with all of the digital work product involved in processing digital evidence. It means that instead of sending a terabyte of retained work product that consists largely of files generated as part of normal processing of digital evidence, but the content of which is not relevant to the issues, I can send only the information that actually pertains to the matter at hand.

My summary opinion

These changes save time and money for competent experts on all sides, reduce many misimpressions that might otherwise result, allows far better and more rapid communication, and reduces the complexity of efforts of experts who can do things the way they feel most productive and effective. At the same time, they force experts to provide what the other side needs to get at the real issues in the case, and will likely increase the reliability and quality of digital forensics ans the results put forth in court. In summary, I like these changes.

