I recall, years ago, putting myself through law school by programming computers. We had no concept, then, of the Internet, which was far away in the future. We didn’t use e-mail, obviously. Later, as a lawyer, I recall interrogatories and document requests that filled whole rooms or even warehouses with paper, but at least we knew what to do with them. The simplicity of those days is long gone. I had my first serious e-discovery experience about five years ago, and for all of the lawyers, it was as though we had all landed on a different planet.

The Federal Rules had not yet come into being, to create the great divide in e-discoverability, with items that can be easily retrieved becoming discoverable under the usual standards, while difficult-to-retrieve evidence is not usually discoverable unless it meets a balancing test that compares the difficulty of retrieval against the need for the evidence. We were not accustomed, as paper lawyers, to anything quite resembling this dichotomy. Consequently, we fought at length over whether given data had “really” been deleted and whether it was retrievable—somehow retrievable, in ways that electronics experts knew, using techniques that were like magic to us. And the rules still beg some of the same questions. How do we determine the difficulty of retrieval? How do we prove it? How do we determine the need for evidence that, after all, is not available and that therefore is unknown, making it difficult to determine the need for it? The answer, of course, is that we rely upon various kinds of data processing experts much more than in the past. These experts become not just sources of information, but guides to guesses about whole categories of information we can get or must retrieve.

Back in the old days, we were only dimly aware of the issue of spoliation. Under today’s rules, upon the filing of a lawsuit, or sometimes even upon the arising of a potential controversy, the parties immediately and automatically become bound to carry out various duties of preservation. But back then, we wondered about that. “Do we need
to tell our people to keep all this stuff?” We were familiar, from the past, with the idea of court orders that required us to preserve evidence, but we had encountered a new world, one that possibly required us to be proactive without a court order. We struggled to project what the litigation might be about, but we did not know, back then, to instruct our clients, firmly, to set aside their usual data destruction policies and act so that we preserved what was relevant. Today, the penalty for failing to do so may be that the jury will receive an instruction that becomes a virtual directed verdict against our client, saying that missing e-documents can be treated as supporting the opposing party. This is an area, too, where some of the major questions are still unanswered, where lawyers have to guess, and where development and redevelopment are constant.

Then, there was the problem of privileges and immunities—a problem that was no less strange. We kept finding privileged and unprivileged documents intertwined in ways that probably would not have happened with paper documents. Separating business advice from legal advice, for example, required more effort than we were used to. And inevitably, there were instances of inadvertent disclosure, more frequently than in the past, as well as of situations in which the legal advice was so intertwined with the discoverable information that one could not be disclosed without the other. All of these issues have undergone fundamental changes, with more changes—and then, still more—to come.

We were clueless about the issue of proof by e-evidence. In principle, I think we thought that this was an easy issue; we would just treat electronically generated documents the same way we would treat paper ones. But the evanescence and mutability of electronic documents changes the picture. Take the original writing (or best evidence) rule, for example. It might seem reasonable to say that a series of electronic impulses makes a document, and the resulting printout is an “original.” But is it really? Documents of this kind can be altered in ways that do not leave a trace. In fact, this is one of the attractions of the electronic medium: the ability of a writer to turn out reams of documents based on a template, with each one differing slightly from the next. In such an unstable world, it dawned on us that we would have to develop a new explanation of the original writings rule. Then there was the even more difficult issue of authentication. What did it take to
put the series of electronic clicks that made up a received e-mail properly into evidence? The same instability of the medium made it more difficult to pin down rules for establishing the authenticity of e-documents. We finally figured out that we might be able to use a “custodian” of the electronic system as our primary witness, but we would need a team of systems engineers standing by just in case. I know that lawyers still find themselves in the same doubtful position, sometimes, but with more confusing law to contend with.

It gradually dawned on us that the function of experts would change in major respects when we handled e-evidence. We might have needed our systems engineers to explain to the jury the limits of available information, or even to interpret some of it. These tasks were different in character from the testimony required of the usual expert.

Fortunately, we settled the case, probably in part because both sides faced such difficult questions in figuring out what we could discover and prove. And although there is more law in this area now than before, the open questions are still there. And the answers, though they keep changing, can be better understood, thanks to the advice given by Paul Rice in this volume.

—David Crump
John B. Neibel Professor of Law
University of Houston