Introduction

After digital information is obtained in discovery, how does one get such information admitted into evidence? Must one lay a foundation? If so, how and what are the governing rules? How might you keep digital information out of evidence? And is that realistic, given the existing scheme regarding admissibility? But if there is a way to do it, don't you want to know your best arguments?

And what if the digital information is hearsay? Did a "system" make a statement, without any person being involved? How does one address the hearsay rule in such a situation? How does one exclude such evidence as not fitting any hearsay exception? Are there legal arguments? Are there foundations that must first be laid? What is the developing law?

Accordingly, this book explores the admissibility of digital evidence.

THE WEIGHT OF THE EVIDENCE

But admissibility is not everything. There are other evidentiary concerns, indeed, which are probably far more important to the practitioner than admissibility. One of these is the *weight* of the evidence—the dynamic whereby the fact finder compares information to determine what fits into his mental construct, and what is rejected, and thus falls away.

Accordingly, this book is useful to litigators doing their jobs long before any trial process. A litigator must know how to ask questions of the information he receives in discovery. All the while, he analyzes the evidence because its authenticity and persuasiveness are his critical raw material—his force and power and the salvation of his client. It is this dynamic of *weight* that he uses to "build a case." Building a case is overwhelmingly fun—a creative process of the highest order. And the stakes are high: In our system, litigation lawyers not only build cases, they build *opposing* cases—antithetical mental constructs unleashed to annihilate one another. In our ancient ritual, litigation field marshals try to outflank each other. They unravel, unzip, disassemble, dissolve, and implode each other—quite suddenly, in many instances. The pop each other's conceptual bubbles. The way they do this is through the weight of the evidence. And in 98 percent of the cases, they do this long before any trial process.

Accordingly, litigators must know how to make digital evidence persuasive. Equally, if not more important, they must know how to *test* digital evidence when it threatens their case. If they know what they are doing, they can launch a crushing flank attack on the opponent. Such information is invaluable to an advocate.

NEW FOUNDATIONS

But in order to do any of this, we must ask, "What are the foundational bedrocks?" What are the new modes of reasoning, the new logic? How do we arrive at a trusted idea like "this is authentic," but with regard to new types of information that defy old paradigms? How do we either establish elements or point out they are missing?

Quite simply, how can lawyers of the new millennium do their jobs without understanding basic concepts about digital evidence? Without an understanding of how to test, prove, or attack the information of our new age, aren't lawyers mere ghosts of the past? Where should we test and probe, and where do we shore up? Do we understand the new information well enough to do these traditional jobs?

Digital evidence needs questioning like all evidence, but a new and different sort of questioning is in order, and this book points out where to begin one's thinking. This is a key part of our professional skill set from this point forward. If we abandon our role as society's experts in information, we loose our power and importance—our righteous calling as the high priests of information. This book is thus a call to a new professionalism.

JUDGES, PROFESSORS, AND STUDENTS OF THE LAW

But certain cases do go to trial, and it is those cases that become the showcases. It is those cases that make the law as it co-evolves with an ever-changing culture. In these cases, judges in the U.S. make rulings on admissibility. Decisions about admissibility have been trivialized of late, as judges were disempowered by the codification of evidence law and the strict rationality tests chosen to guide admissibility. But armed with a new awareness, thinking judges might now reconsider their habitual admissibility determinations—including the foundations necessary to properly authenticate digital information or qualify statements of information systems as reliable.

But in addition, increasingly in the United States and overwhelmingly throughout the world, judges and magistrates are the organs giving weight to evidence. Judges thus need to understand the new dynamics as well as any members of the profession. If they are considering digital information, they need to understand what they are weighing and how to weigh it.

Law students and their professors may read this book. They are the future of the profession, and in this instance we discuss nothing less than disputes being decided on true facts. And the book may be of interest to evidence scholars. It somewhat unabashedly throws down an intellectual gauntlet. It hints at a new scheme. Concepts underpinning many of the law's most basic assumptions are questioned. The book suggests some of these are now outdated, perhaps even the most important ones. And longstanding psychological constructs, adopted by our culture and legal system both, are implicated, and

the book therefore tries to take its readers on a journey of sorts—outside their normal modes of thought.

In short, law is evolving at the start of the new millennium. We are at a crossroads—a change of phase. With our new information infrastructure, the concept of written evidence has reached a critical tipping point. Judges, professors, students, and thinkers must rewrite the rules. When something so important to civilization as writing suddenly morphs into a new system, the world's institutions, but particularly its legal systems, simply must adapt.

RELEVANCE TO BUSINESS AND INFORMATION GOVERNANCE

But foundations for digital information are essential to far more than litigation. Litigation is the resolution of unfortunate problems—an exception, one hopes, to the smooth operation of society. Businesses still need to think about these issues so they can properly create and handle the information of their enterprises. Unless business lawyers advise their clients how to handle information so as to establish proper foundations, a company's records will be suspect. They will be compromised, or become worthless through lack of provable authenticity. Increasingly, federal schemes mandating certain provable characteristics about information will require businesses, and their advisors, to understand digital information. We see such schemes arising in health care, the financial sector, and in publicly traded companies. Without an understanding of the new foundations, complying with rapidly evolving substantive law about digital information will not be possible.

For example, if a businessperson is required to prove that a digital file was not edited during the last five years, how does she know how to do that? Is she currently, given her setup, even capable of doing it? How can she test whether a certain person really "signed" something, if the information is digital? How can she know when something happened, and trust that it is an accurate time she is using? We provide case studies to demonstrate these challenges, and show how certain businesses have already met them successfully.

One function of this book, therefore, is that it provides a road map about how information's design and implementation by industry, government, and citizens must henceforth evolve so as to provide good "information governance." There can be no solid foundation underlying authentic informational records unless systems record enough data to allow testing for certain attributes. Overwhelmingly, our current systems lack good information governance, and we therefore cannot test for truth in relevant areas. We are relegated to consideration of the sloppy circumstances. Sometimes there is good information, but most of the time there is not. We are adrift.

But this book points out there are ways to design regimes of information that give "strong" knowledge, tantamount to a "demonstration," as the first evidence scholars called it. There are digital information schemes that allow one to have strong tests for authenticity, integrity, identity, and time. There are even ways, using such schemes, to recreate the concept of an original document. Accordingly, management of information needs to co-evolve in accordance with our new understanding of writing forms and the new-age written record. This is the coming revolution in the world of business records

that will unfold over the next two decades. As explained in this book, we must evolve towards *eunomia,*[1] or good information governance in societal records.

RELEVANCE TO SOCIETY'S LARGER SEARCH FOR TRUTH

The book is also relevant to the larger society. The word "evidence" is a legal word, but at the same time it is also an everyday word used by laypeople. What is the evidence? What is the truth? Citizens will always ultimately demand an ability to learn the truth about the past—whether it be an historical event, a government scandal, or the facts of a personal matter. In the United States, we certainly assume a citizen's power to get at the truth is something our society values and will not lightly discard.

A presumption of this book is that the twenty-first century wants and deserves a skill set empowering the discovery of truth. Thus, the observations here are of value to an emerging intellectual fabric. Society must come to grips with whether it currently has an ability to learn the truth about everyday communications, agreements, transactions, and indeed all types of records of digital information. As explained below, we currently exist in a regime of *untestability*. Can society empower its citizens, historians, and auditors? Or must written assertions be taken on faith?

Society henceforward needs new skills, and a new understanding, for a new age of information.

THE CONSEQUENCES OF NEUTRALITY

In the 1990s certain states, most notably Utah and Washington, but also to some extent California, began legislating technological specifications for digital evidence records. But during 1999 and 2000, a strong movement of "technological neutrality" appeared in U.S. law. This started with the 1999 Uniform Electronic Transactions Act (UETA), published by the National Conference of Commissioners on Uniform State Laws (NCCUSL). The Act defined an "electronic signature" as "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." The UETA Comments made clear that anything electronic would suffice—from a mere "click" in a Web browser, to a recording of a voice on an answering machine, and so on. "Electronic records" were similarly technologically generic. Accordingly, generally under UETA as a matter of substantive law, any type of digital information could be either a signature or a record, with the totality of all the circumstantial evidence—digital and real world both—being relevant and necessary.

This neutrality policy was made a matter of preemptive federal law in the Electronic Signatures in Global and National Commerce Act of 2000 (E-SIGN").[2] Under Section

1. "Good order," after the Goddess of order and good governance in Greek mythology, Eunomia.

2. UETA and E-SIGN did create the potential for resurrecting the concept of a digital original. See, e.g., 15 U.S.C. § 7201, which sets forth definitions and requirements for such things as "control" and a "single authoritative copy" of transferable records. In her Case Study in Appendix B, Grace Powers illustrates how the mortgage industry worked with these E-SIGN and UETA concepts, which in turn correlate to certain requirements in the Uniform Commercial Code, to create digital "originals" that can be bought and sold on markets.

101 (a)(2)(A)(ii) of E-SIGN, 15 U.S.C. § 7002 (a)(2)(A)(ii), there is an exception to preemption by the technologically neutral E-SIGN "only if" a state statute, rule, or regulation does not specify procedures that require or accord greater legal status to specific technologies or technical specifications. The United States thus became substantively "technologically neutral" with regard to digital evidence on October 1, 2000, the effective date of E-SIGN. We are in a wide-open, "anything goes" world of digital information.

Accordingly, this book includes a discussion of digital evidence regimes in five other nations—Argentina, France, Germany, Japan, and the Russian Federation—not only to show the international relevance of these issues, but also to highlight how the United States is in the minority position worldwide. By contrast to the U.S. policy of technological neutrality, other countries have already embraced certain of the eunomic solutions we discuss here, as a matter of substantive law, and either mandate them or give them the benefit of presumptions in dispute resolution and commerce. In short, other nations have done what certain of the states in the United States started doing back in the mid-1990s until the neutrality policy was implemented in 2000.

Because our law does not legislate information regimes for interactions among citizens, but allows them to use any type of digital information and security procedures they choose, we in the United States must become expert in understanding the differences implicated by different information regimes. We therefore analyze information in its mode as evidence, and it is through the law and topic of evidence that we must address the issues in this book. Our policies mean we must understand the reality of the new information. Everyone here has a choice, and different schemes allowing different types of proof are used freely. It seems safe to say there will always be a need to get at the truth no matter what regime of information is involved.