

# INTEGRITY, SECURITY AND ADMISSIBILITY

by Al Harrison

## I Electronic Evidence

### A. Nature

1. Composed of electrical impulses: Binary Digits (“bits”)
2. Stored on Suitable Media as Strings of Bits: Files and Databases
3. Invisible to the Human Eye
4. Susceptible to Transformation and Corruption

### B. Integrity

1. Naked or “blanketed” or coded or concealed
2. Read or Write Protection; passwords
3. Encryption
4. Backups and Archives
5. Deletion & Shredding
6. Chain of Custody

### C. Discovery

1. Broad Discovery Rules encompass Electronic Evidence
2. Scope & Access: Hardware, Networks, Software
3. Protective Orders & Agreements
4. Spoliation: Traditional Remedies; *Trevino v. Ortega*
5. Demand for Retention of Stored Electronic Evidence

## II Authenticity & Admissibility of Electronic Evidence

### A. Origin of Information Stored in Files & Databases

1. Source of Evidence
2. Software: Mass Market or Custom
3. Requisite Platform

B. Thresholds for Authentication

1. Reasonable Exchange: *Am. Bankers v. Caruth; Williams v. duPont*
2. Electronic Format: *Nat'l Union Elec. v. Matsushita Elec.*
3. Trace Transformations of Underlying Information
4. Custody & Control
5. Electronic or Digital "Signatures"

C. Admissibility

1. Witness Identification of Evidence
2. Available Formats of Evidence
3. Viewing by Judge & Jury
4. Regularity of the Electronic Evidence
5. Demand for Retention of Stored Electronic Evidence

III Security Measures

A. Data Protection Protocol: Files, Databases, Storage Media

1. Passwords
2. Anti-virus Shield
3. Encryption
4. Retention Policy: Shredding
5. Backup Policy
6. Segregation of Confidential Information (Avoid Inadvertent Disclosure, Waiver of Attorney-Client & Work Product Privilege)

B. Internet Access

1. Firm-Wide Policy
2. Approved Activities (E-mail and Web Browsing)
3. Disapproved Activities (Chat; Download Restrictions)
4. Electronic Trails of Net Activity
5. Firewalls for Controlling Entry to Firm Intranet

C. Beware of E-mail Frailties

1. Knee-Jerk, Informal Responses
2. Distribution & Publication Path Unknown
3. Delay Sending All Outgoing E-mails
4. Selectively Read Incoming E-mails
5. Safeguard Client Confidential Information & Work Product
6. Usually not Transitory

