



**PARTNERS**

***The Negligent Spoliation of Electronic Information: Practical Advice  
for Successfully Preserving Digital Data.***

Presented By Dean Gonsowski, J.D., CISSP  
Managing Director, S3 Partners

# *Omnia Presumuntur Contra Spoliatorem, ...*

---

- ... meaning "all things are presumed against a despoiler or wrongdoer."
- ... meaning that your case is in a lot of trouble if the court finds that your client has intentionally **or unintentionally** destroyed electronic evidence

# Outline

---

- Spoliation Penalties
- The Preservation Mandate
- Triggers of the Preservation Duty
- Negligent Spoliation
  - ✓ The initial handling/preservation of electronic evidence
  - ✓ The ongoing use of computer systems
  - ✓ Turning off presumptively valid document retention/destruction policies
- Creating a Defensible Preservation Effort
  - ✓ What's being preserved?
  - ✓ How much is being preserved?
  - ✓ How to successfully communicate the effort?

# Penalties

---

Sanctions for the spoliation of evidence include:

- ✓ adverse inferences or presumptions (at either the case or issue level),
- ✓ preclusion of evidence (including preclusion of expert or other forms of testimony),
- ✓ monetary sanctions,
- ✓ dismissal,
- ✓ default judgment, or
- ✓ the granting of summary judgment in favor of the prejudiced party

# Source of the Duty to Preserve

---

- The origin of the duty to preserve potential evidence arises from both common law and the A.B.A. standards.
- “When a lawyer who has been retained to handle a matter learns that **litigation is probable** or has been commenced, the lawyer should inform the client of its duty to preserve potentially relevant documents and of the possible consequences of failing to do so.”
- This obligation to preserve applies equally to “information contained or stored in an electronic medium or format, including a computer word-processing document, storage medium, spreadsheet, database and electronic mail.”

*ABA Civil Discovery Std. 10 & 29(a)(i) (1999)*

# Triggers = Reasonable Notice

---

- The Court's authority to sanction a party for failing to preserve documents is both inherent and statutory (FRCP 37)
- Either way, the first step is to determine whether the alleged spoliator was under **sufficient notice** to preserve information
- Unfortunately, the “trigger” of that duty is often unclear, and may apply at any of several stages:
  - ✓ Prior to Complaint (e.g., Demand Letter)
  - ✓ After Complaint
  - ✓ After Protective Order
- Notice of “What?”

# Negligent Spoliation -- Handling/Preserving Evidence

---

- Simply turning on a computer alters a number of files; potentially spoliating the digital evidence
- Opposing experts/counsel may argue that this alteration removes the back-up copy from the scope of FRCP 1001(d), which holds that copies are admissible to the same degree as an original
  - ✓ Chain of custody
  - ✓ Authentication
  - ✓ Ghost Images vs. Bit-for-Bit Images
  - ✓ Read-Only copies

# Negligent Spoliation -- Continuing to Use Systems

---

- “Deleted” files are not really deleted, since when a user “deletes” files the computer system merely marks that area on the hard drive as being “open” for the writing a another file.
- The ramifications of this reality, forensically, is that “deleted” files remain recoverable within a system for a period of time, until the computer needs the space to write a new file. Only then is the “deleted” file actually destroyed.
- In *Antioch v. Scrapbook Borders, Inc.*, the court recognized this fact by stating that

“... the Defendants may have relevant information, on their computer equipment, which is being lost through normal use of the computer,...”
- Ramifications? Costs?
  - ✓ Imaging
  - ✓ Quarantine
  - ✓ Snapshots of Data

# Negligent Spoliation -- Stopping Document Destruction Systems

---

- Courts have nevertheless upheld the validity of “**bona fide, consistent and reasonable**” document destruction policies, even where these policies ultimately destroy evidence relevant to litigation
- Admonishing the defendant for negligently failing to preserve evidence, the *Court in Lewy v. Remington Arms Co.* concluded that “a corporation cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy.”

# Negligent Spoliation -- Stopping Document Destruction Systems

---

- Back-up Tapes
  - ✓ Re-circulation
  
- User-specific systems
  - ✓ Decommissioning
  - ✓ Selling
  - ✓ Upgrading
  - ✓ Swapping
  - ✓ New software
  - ✓ “Anti-forensics” Activities
    - Defragmenting
    - Wiping (*Kucala Enterprises v. Auto Wax*, No. 02C1403 (N.D.IL. May 23, 2003)).
    - Reformatting

# Creating a Defensible Preservation Plan:

## 1) *What's being preserved?*

---

- After performing an assessment of the client's IT systems and software you can then create a preservation strategy that focuses on:
  - ✓ Custodians
  - ✓ Departments
  - ✓ Data types (Active, Archival, Forensic, Paper)
  - ✓ Product lines
  - ✓ Software types
  - ✓ Physical locations
  - ✓ Date ranges
  
- Fortunately, while the duty to preserve evidence is a broad mandate, it does not require a litigant to keep every scrap of paper or electronic document.

# Creating a Defensible Preservation Plan:

## 2) *How much is being preserved?*

---

### ■ Cost

- ✓ Technology
- ✓ Tools
- ✓ Implementation
- ✓ Oversight
- ✓ Lost Productivity

### ■ Benefit

- ✓ Reduction of potential spoliation penalties, which should be contrasted against the amount in controversy
- ✓ “Clean hands,” which should allow more vigorous discovery demands

# Creating a Defensible Preservation Plan:

## 3) *How to successfully communicate the effort?*

---

- The corporation should caution employees that any deliberate violation of promulgated guidelines could result in serious disciplinary action, up to and including termination and sanctions provided for by the Federal Rules of Civil Procedure, civil contempt for violation of an Order of the Court, or criminal contempt pursuant to 18 U.S.C. § 401(3)
- The corporation should notify employees how to report evidence of document destruction, for example, through the use of a telephone hotline
- The corporation should provide the names and telephone numbers of individuals to contact in the event that questions arise about document retention, and designate a primary contact source for information about document preservation
- The corporation should create “uniform” guidelines that represent the systematic process necessary to preserve documents, and identify the circumstances when a document may be discarded and the procedures to be employed
- The notice to employees regarding document retention should be in emboldened or enlarged font to draw attention to the importance of the notice
- The corporation should prepare and utilize a document destruction index
- Distribution via email may not be sufficient, especially if all employees do not have access; regular mail may be necessary
- During oversight and implementation, the corporation shouldn't use a lay person to spearhead the effort



**PARTNERS**

Dean Gonsowski, J.D., CISSP  
[dgonsowski@s3partners.com](mailto:dgonsowski@s3partners.com)  
Managing Director, S3 Partners  
Denver, Colorado  
303.433.6371