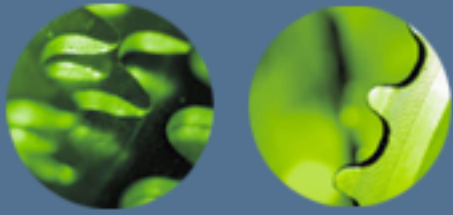




# COMPUTER FORENSICS: REAL WORLD CASES

Evelyn J. Furse  
Senior City Attorney  
Salt Lake City Corporation

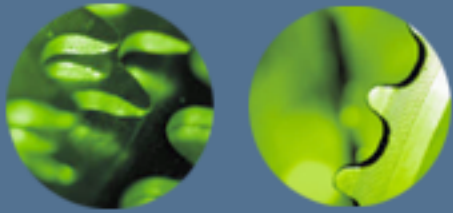


- This presentation is educational, not legal advice and cannot substitute for advice of counsel.



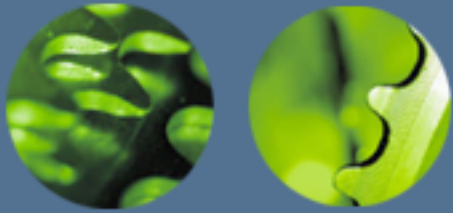
# BACKGROUND





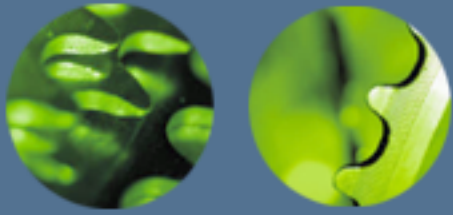
## Electronically Stored Information (ESI) is . . .

- “Any type of information that is stored electronically”
- “[B]road enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments.”
  - FRCP 34 Advisory Committee Notes re 2006 Amendment Subdivision (a)



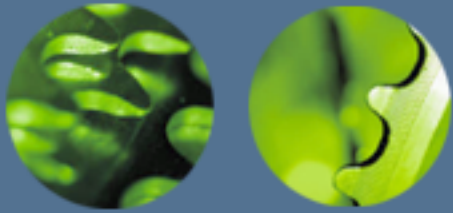
## ESI includes . . .

- Word Processing Documents
- E-mail
- Spreadsheets
- Calendaring programs
- Databases
- Photographs
- Time records
- Payroll records
- Presentations
- Voice mail
- Audio Recordings
- Music files
- Text messages
- Instant messages
- ***Metadata***



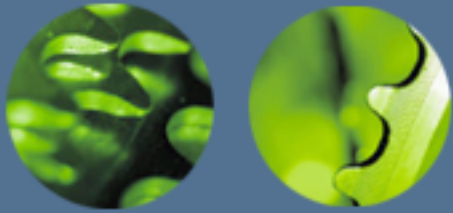
## Metadata is . . .

- Data about data
  - i.e. information about who created a document, when, how big it is, who changed it, when, changes made to the documents, deleted notes, etc.



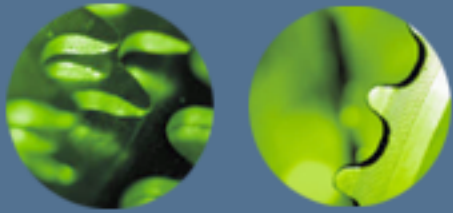
# Places Where Electronic Data Lives . .

- Network Drives
- Servers
- Desktop Computers
- Laptop Computers
- MDTs (Mobile Data Terminals)
- Discs
- CDs
- DVDs
- Flash/USB/Jump Drives
- Databases
- Telephones
- Blackberries/Personal Digital Assistants (PDAs)
- Voicemail Systems
- Fax machines
- Copy machines
- Cars
- Parking Lot control devices
- Internet/Intranet Sites
- Back up Tapes
- Archives
- No longer used systems, hardware & software
- Disaster Recovery Devices
- Home Computers
- Personal E-mail Accounts
- With your Agents



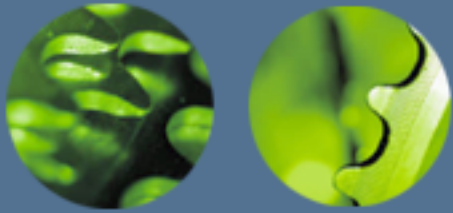
## Why you care . . .

- As Records Managers, much of this may be “records,” and you need to know about it to manage it.
  - AND
- ESI must be produced in all civil lawsuits the same as any other documents.
  - Federal Rules of Civil Procedure changed December 1, 2006,
  - Utah Rules of Civil Procedure changed November 1, 2007,



## How that is different than before . . .

- Rules specifically provide for sanctions against a party if that party does not suspend destruction of any ESI once the party “reasonably anticipates litigation”.



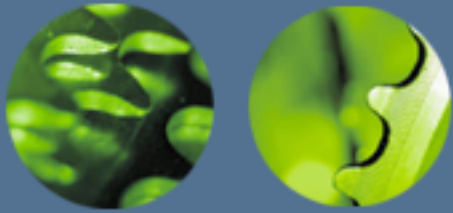
## Destruction Happens Without Anybody Intending.

- Automatic deletion of e-mail according to policy
- Automatic destruction of documents according to record retention schedule
- Altering of ESI by opening documents
- “Defragging” computer
- Some Internet & PC Privacy Protection Programs
- Computer Crash



## Possible Sanctions Include . . .

- Pay opposing counsel's fees . . . \$\$\$
- Orders to produce more data . . . \$\$\$
- Orders to recover data . . . \$\$\$
- Monetary penalty . . . \$\$\$
- Adverse inference instructions . . . \$\$\$
- Finding of facts against you . . . \$\$\$
- Exclusion of your evidence . . . \$\$\$
- Dismissal of Case/Claim or Entry of Default \$\$\$
  - » FRCP 37(b)(2); URCP 37(b)(2)



## What to do if you anticipate litigation . . .

1. Suspend all destruction of all relevant or possibly relevant documents including ESI.
2. Secure existing documents and ESI.
3. Determine what is reasonably accessible.



What to do now to be able to do those three things . . .

## 1. Create an ESI team, including:

Decision maker

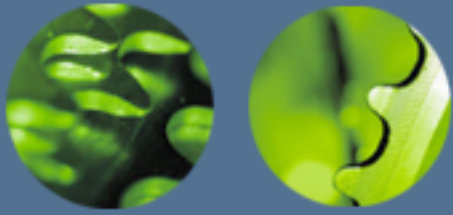
IT/IMS—Tech person with authority

IT/IMS—Front line tech person

In-house Attorney (and/or outside counsel)

Records Manager(s)

Others—representative of dept., HR . . .



## 2. Create/Review Record Retention Policy explicitly including ESI

Policy should “make sense” from a business case, not from the point of view of avoiding record retention.

Ensure all employees including new hires KNOW the policy.

Policy must be followed, monitored, and enforced.

Understand possible ways ESI can be eliminated and avoid detection. Are there ways to “plug” these holes?



## Key Points for Retention Policy

- Define ESI with examples in your business.
  - Policies for ESI should follow those for hard documents—the base concept is the same.
    - i.e., If invoices are worth keeping for 2 yrs., electronic invoices are worth keeping for 2 yrs.
- Define what is automatically deleted and when.
- Provide guidance on who has authority to delete and when.
- Differentiate between the wheat and the chaff.
- Create obligations.



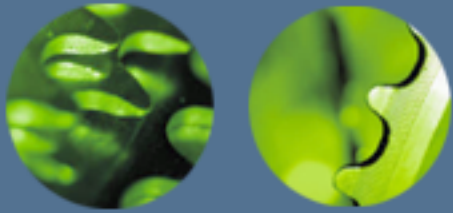
## Consider prohibiting

- Adding programs to computer without permission
- Instant messaging
- Saving documents to disc, jump drive (or register such with IT dept)
- Use of personal computers for work (or register such with IT dept)



## Possible Elimination

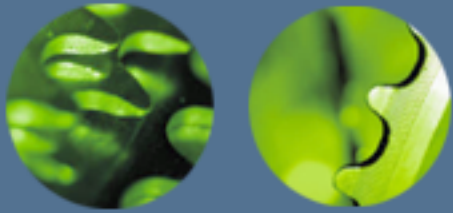
- E-mail users can eliminate ESI by “double deleting”—deleting e-mail and deleting e-mail garbage the same day the e-mail is sent/received.
- One way to address this issue is to “journal”. Employ a system that saves all e-mail to back-up upon sending/receiving.



### 3. Inventory your hardware and software.

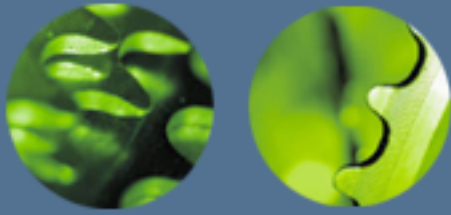
Create a list or map or diagram of all of the company's software and hardware in use by person or location or, ideally, both.

Create a list or map or diagram of all of the company's software and hardware not in use, but retained.



## 4. Understand the Company's back up system.

- How are back ups made
- When
- How are they used
- How long are they retained
- Are there ways in which ESI might accidentally avoid back up
  - i.e. leaving the computer on overnight
  - Can you “plug” these holes?



## 5. Create a Written Litigation Hold Policy

What events will automatically trigger a litigation hold?

What events might trigger a litigation hold?

ESI team meets when? Who convenes? Back up?

What are factors for consideration?

If hold imposed what actions will be taken by whom?

list of issues, list of people, list of possible locales of ESI and hard documents

today, tomorrow, this week, follow up



## SAFE HARBOR

If you have and follow a records retention policy,  
and

You institute a litigation hold when you reasonably  
anticipate litigation,

“Absent exceptional circumstances, a court may  
not impose sanctions under these rules on a  
party for failing to provide electronically stored  
information lost as a result of the routine, good-  
faith operation of an electronic information  
system.” FRCP 37(f), URCP 37(g)