



ATTORNEY GENERAL OF TEXAS  
GREG ABBOTT

# GTC Southwest eDiscovery and Government Records: What You Need to Know

David G. Halpern  
Assistant Attorney General  
February 18, 2010



December 1, 2006

- ▶ Amendments to the Federal Rules of Civil Procedure Go into Effect



## Why Should You Care?

- ▶ Litigation is going paperless  
→ “electronic discovery”
- ▶ Data is evidence
- ▶ Evidence must be preserved



## Recent Data

- ▶ With approximately 30 billion e-mails created or received by federal government agencies each year,
- ▶ Probably close to 100 billion e-mails are sent daily...
- ▶ ... at least 25% of which have one or more attachments of varying length.



▶ 1 in 4 recently reported cases involving eDiscovery involved SANCTIONS,

- Per National Association of Attorneys General
- Citing Kroll Inc. study of 138 cases
- January 1, 2008-October 31, 2008



# The Net(work) Effect of the New Rules

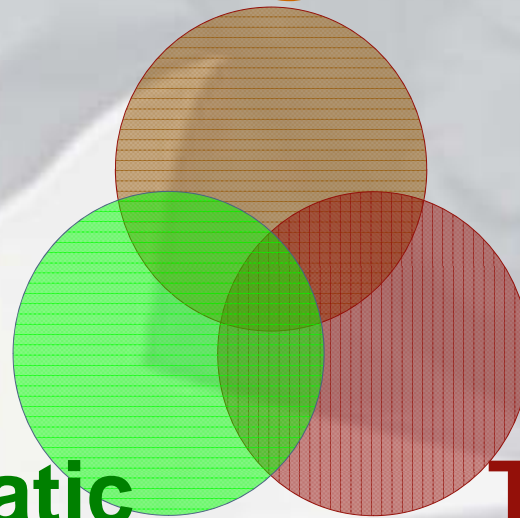
## New and Better Clarified Duties

- For counsel
- For courts
- For clients, which includes:
  - Administration
  - In-house counsel
  - Staff
  - **IT**



# Oh, My! The New Reality

Legal



**Programmatic**

**Technical**



# What Data Needs to be Preserved?

- ▶ All forms of electronic communications – e.g.,
  - e-mail
  - word processing
  - calendars
  - voice messages
  - instant messages
  - spreadsheets
  - videos & photographs
  - information in PDA's
  - and data in any other locations where electronic information may be stored



# The New Rules

- ▶ Contemplate the suspension of routine or intentional
  - purging,
  - overwriting,
  - re-using,
  - deleting, or
  - any other destruction of electronic information relevant to a lawsuit, wherever it is stored.
- ▶ At a work station, on a laptop, or at an employee's home



- Information must be preserved in its original electronic form, so that all information contained within it, whether visible or not, is also available for inspection.
- It is NOT sufficient to make a hard copy of electronic communication.



## Are My Personal Devices Included?

- ▶ YES, when used for official business.
- ▶ This will make the IT job more complex if asked to place litigation hold on computers outside of your control.



## How IT Can and Must Help

- ▶ **You will direct or assist your** office's effort to:
  - identify and
  - preserve
  - all potential sources of electronically stored information in your possession or under your control.



## Controlling Costs

- ▶ IT can and must quantify costs
  - To acquire tech solutions,
    - Software
    - Backup tapes
  - In manpower
    - To implement a preservation effort
    - To identify ESI
    - To gather and organize ESI
    - To review ESI for Privilege and Confidentiality
    - To produce ESI



## How will I(T) know when this duty is triggered?

- ▶ IT should be advised of the duty to preserve electronically stored information through a notice.
- ▶ This is called a “**litigation hold**” (or “**preservation hold**”).



## Duty to Preserve

**Party is under a duty to preserve information when**

- ▶ Litigation is pending, or
- ▶ Litigation is “**reasonably anticipated**”



## Duty to Preserve

### When Under the Duty to Preserve, “Litigation Hold” Kicks In

- **Intervention** in routine operation of information system, i.e., document retention plan.



## What if the information or system is remote or arcane?

- It's unclear if good faith requires prevention of data loss of information
  - ▶ that the party believes is not reasonably accessible
  - ▶ To be decided on case by case basis



## What about policy for auto delete of files from e-mail or the network?

- ▶ When a litigation hold is imposed IT must ensure compliance--→
- ▶ Endeavor to preserve all records and data identified by the hold.



## May employees remove data from computers or the network?

- ▶ Yes, if they know that:
  - It is not the subject of the litigation hold; and
  - Removal is consistent with policy.



## What happens when an employee leaves employment with the State?

Employment transitions are no excuse.

- ▶ Steps must be taken to preserve and protect data and information in all forms
- ▶ As required by your record retention policies, and
- ▶ As required by law.
- ▶ Special attention is essential when a litigation hold is in place.
- ▶ **ONGOING MONITORING IS A MUST.**



## Who decides what data or information will be produced?

- ▶ Collaboration is the key
- ▶ Legal counsel will produce responsive ESI
- ▶ In coordination with those who:
  - Created
  - Retained
  - And/or retrieved the information  
(GENERALLY **IT**)



# A new intersection of law and technology



- ▶ ESI is subject to inspection & testing
- ▶ Information systems are, too
- ▶ WHY?
  - To insure integrity of the ESI that is produced
- ▶ THE CONSEQUENCE?
  - IT personnel are subject to scrutiny
  - You may give testimony under oath
  - As a person with facts relevant to discovery



## A Slippery Slope on the Horizon

- ▶ Questions invite assertions of privilege
- ▶ And the need to be aware of the possibilities that some communications may/not be privileged



## Rules on the Run

- ▶ Don't need to learn 'em
- ▶ But, you may want to know the big ones
- ▶ To know how they will affect your life



# Initial Disclosures

## A PARTY MUST

- Without waiting for a discovery request;
- Provide a copy or description;
- By **category** and **location**;
- Electronically stored information;
- Which may support a claim or defense
  - ▶ Unless solely for impeachment Rule 26(a)(1)(B):



Disclosure must be made  
within 14 days of Rule 26  
conference

You must be prepared to address and/or provide:

- A copy of description by category and location
- All Electronically Stored Information
- That may support a claim or defense Rule 26(a)(1)(B)



“A party need **not** provide discovery of electronically stored information

- From sources. . .not reasonably accessible
  - ▶ Because of **undue burden** or **cost**”
- Unless, and upon a showing of burden/cost
  - ▶ Good cause is found
  - ▶ Consider cost sharing
  - ▶ RULE 26(b)(2)(B)



## \$Cost Sharing Factors to Consider

- ▶ Specificity of the request
- ▶ How narrowly tailored it is
- ▶ The relative cost of production vs. damages at issue
- ▶ The relative wealth of the parties
- ▶ Alternatives to the evidence sought



## Claims of Privilege or Protection

- The so-called “Claw back” aka oops rule
  - ▶ ....so, can I please have it back?
- Receiver must:
  - ▶ Return,
  - ▶ Sequester, or
  - ▶ Destroy
  - ▶ **OR PRESENT THE INFORMATION TO THE COURT UNDER SEAL Rule 26(b)(5)(B)**



## Practice point

- To reduce cost and delay in risk avoidance
  - ▶ Parties may minimize the risk of waiver by agreement or protocol



## Rule 33: Interrogatories

- ▶ Business records expressly includes electronically stored information
- ▶ “...in sufficient detail to permit the interrogating party to:
  - **locate** and
  - **identify**
- ▶ as readily as can the party served, the records from which the answer may be ascertained.”



## Rule 34: Production

### Of Documents, Electronically Stored Information, and Things

- Rule 34(a): party may
- inspect
- copy
- test or
- sample electronically stored information...
  - ▶ Including other data or data compilations stored in any medium
  - ▶ From which information can be obtained-translated, if necessary, by the respondent
  - ▶ Into reasonably usable form. . . .



## Testing & Sampling

### Now expressly authorized

- This includes the ESI that is produced AND
- The electronic information SYSTEM
  - ▶ Opening up the door to matters that may be
  - ▶ **Confidential** or **Privileged**



## Rule 37: Sanctions

### FAILURE TO MAKE DISCLOSURE OR COOPERATE IN DISCOVERY

- “Absent exceptional circumstances, a court may not impose sanctions...for failing to provide electronically stored information lost as a result of routine, good-faith operation of an electronic information system.”

- AKA THE

**SAFE HARBOR**

- BUT.....BEWARE



## Below the Calm Waters of the Harbor

- Good faith means a party is not permitted to **exploit the routine operation** of an information system
  - ▶ **to thwart discovery obligations**
  - ▶ **by allowing that operation to continue in order to destroy specific stored information**
  - ▶ **that is required to be preserved.**



## Applies to Non-Parties

- Duty in Responding
  - ▶ If the subpoena does not specify the form/s for producing electronically stored information
  - ▶ Must produce the information in a form that is:
    - Ordinarily maintained, or
    - Reasonably usable Rule 45



## Texas Rules: 196.4 "Electronic or Magnetic Data"

- ▶ REQUESTING PARTY:
  - Must specify the form requested
  - Must make request specifically
  
- ▶ RESPONDING PARTY
  - Must produce responsive material that is:
    - **That is reasonably available**
    - **In the ordinary course of business**



ATTORNEY GENERAL OF TEXAS  
GREG ABBOTT

Questions





ATTORNEY GENERAL OF TEXAS  
GREG ABBOTT

Thanks,  
and Good Luck