SPOLIATION OF EVIDENCE

Now what do I do?

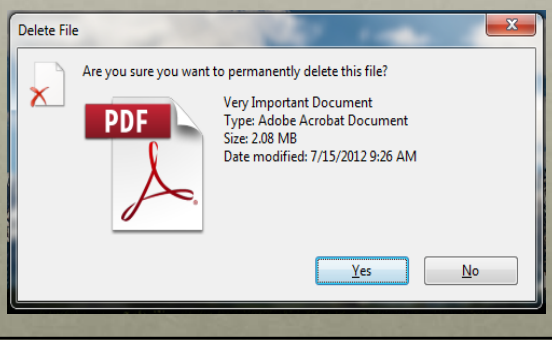
Presentation by: John C. Haas, Esq.
W. Benjamin King, Esq.

LITVAK LITVAK MEHRTENS and CARLTON, P.C.
ATTORNEYS AT LAW

DISCUSSION TOPICS

- **I.** What is Spoliation?
- **II.** What are, *or were*, a party's and counsel's obligations?
- **III.** Minimizing the risk of spoliation or sanctions.
- **IV.** How can we get social media, emails, texts and the like?
- **V.** Can we recover spoliated information?
- **VI.** Judicial Remedies.

I. WHAT IS SPOLIATION?



SPOLIATION DEFINED

Spoliation occurs when a party destroys or materially alters evidence, or fails to preserve property for another's use as evidence, in pending or reasonably foreseeable litigation. *Cache La Poudre Feeds v. Land O'Lakes, Inc.*, 244 F.R.D. 614, 620 (D. Colo. 2007); *Castillo v. Chief Alternative*, LLC, 140 P.3d 234, 236 (Colo. App. 2006)

SPOLIATION DEFINED

- Recognizing the triggering event to preserve will depend on the facts of each case, **"the mere possibility"** of litigation does not trigger the duty. *See*, *Cache La Poudre*, 244 F.R.D. at 621.
- The duty to preserve evidence arises "when litigation is pending or reasonably foreseeable under an **objective standard**, which does not carry a gloss requiring that litigation be imminent, probable, or without significant contingencies." *Micron Technology, Inc. v. Rambus, Inc.*, 645 F.3d 1211 (Fed. Cir. 2011); *Oto Software, Inc. v. Highwall Technologies, LLC*, No. 08-CV-01897-PAB-CBS, 2010WL3842434 at 8 (D. Colo. Aug. 6, 2010) (reiterating an "objective" standard of review).

II. WHAT ARE, *OR WERE*, EACH PARTIES' DUTIES?

Every file?

- A litigant is under no duty to keep or retain every document in its possession, but it must not destroy unique or relevant evidence or that which is reasonably calculated to lead to the discovery of admissible evidence. *Cache Law Poudre Feeds*, 244 F.R.D.at 621 *supra*.; *accord*. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217-18 (S.D.N.Y. 2004).

WHAT ARE, *OR WERE*, EACH PARTIES' DUTIES?

- Colorado Rules of Professional Conduct 3.4(a):

Fairness to Opposing Party & Counsel

"A lawyer shall not: (a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy, or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act…."

WHAT ARE, *OR WERE*, EACH PARTIES' DUTIES?

CRPC 3.4(a), comment 2(c) states:

"…subject to evidentiary privileges, the right of an opposing party…to obtain evidence through discovery or subpoena is an important procedural right. The exercise of that right can be frustrated if relevant material is altered, concealed or destroyed ***…including computerized information***."

III. MINIMIZING THE RISK OF SPOLIATION?

"Preservation Letter"

What is it?

A preemptive letter putting **(a) opposing parties, (b) third parties, and (c) your own clients** on notice that they must preserve evidence, including electronically stored information ("ESI").

When should it be sent?

As far in advance of litigation as possible and, in any event, no later than the commencement of an action.

PRESERVATION LETTERS

As to your own client:

A. Notifies them of the duty to preserve evidence.
- i. Which minimizes the risk of spoliation sanctions against them; and
- ii. Mitigates the attorney's risk of sanctions by the court or a malpractice action from his own client for failure to advise the client of the duty to preserve evidence.

As to the Opposing Party and Attorney:

A. Notifies them to, or "triggers," the duty to preserve evidence; and

B. If spoliation occurs, strengthens your argument for sanctions against opposing party or counsel.

IV. HOW CAN WE GET SOCIAL MEDIA, EMAILS, TEXTS AND THE LIKE?

- A. Preemptive Gathering of Information.
- B. Issuing Subpoenas?
- C. Rule 34 Discovery.
  - 1. Request download of all content;
  - 2. Request a "Release" or "Authorization" from the user to obtain the content directly;
  - 3. Request the user's Password; or
  - 4. Request a Forensic Image of the content.

A. PRE-EMPTIVE GATHERING OF INFORMATION

Hypothetical: *Might the Preservation Letter alert the opposing party to promptly "clean-up" any damaging evidence?*

Pre-emptive and Proactive Gathering of information, means, as early as reasonably possible, proactively review the opposing party's available sources of information.

a. Social Media: FaceBook, MySpace, Twitter, etc.

b. Professional Postings: LinkedIn, business website or advertising.

c. Family Computer.

- There is no prohibition to an attorney accessing publicly-viewable social media, but an attorney cannot misrepresent himself to gain access.

A. PRE-EMPTIVE GATHERING OF INFORMATION

But, John, what if it's ***my client*** who has damaging content? What can I do??

Answer. An attorney may:

a. Counsel a client as to what are or are not appropriate posts or content;

b. Instruct a client to utilize "privacy settings" to remove the content from public view;

c. Instruct a client to "Remove" the damaging content so long as it is preserved for production in response to discovery or other disclosure rules;

d. Advise a client to refrain from using social media or the like altogether during the action;

DEACTIVATING VS. DELETING A FACEBOOK ACCOUNT

- Facebook's current **DELETING POLICY** states *inter alia:*

"If you permanently delete your account:

- a. **You will not be able to regain access to your account.**
- b. It may take up to 90 days to delete all of the things you've posted, like your photos, status updates or other data stored in backup systems. While we are deleting this information, it is inaccessible to other people using Facebook.
- c. Copies of some material (ex: log records) may remain in our database for technical reasons. When you delete your account, this material is disassociated from any personal identifiers."[1]

DEACTIVATING V. DELETING A FACEBOOK ACCOUNT

Facebook's **DEACTIVATION POLICY** states:

- "You can deactivate or delete your account at any time."
- You may deactivate your account for any number of temporary reasons. This option gives you the flexibility to leave and come back whenever you want. If you deactivate your account:
- People won't be able to search for you or see information on your Timeline.
- Some information, like messages you sent, ***may still be visible to others***.
- "***We save the information in your account*** (ex: friends, photos, interests), just in case you want to come back to Facebook at some point. ***If you choose to reactivate your account, the information on your profile will be there when you come back.***"

B. ISSUING SUBPOENAS?

Question:
Can't we just serve subpoenas on FaceBook, Google, Yahoo, MySpace and the like?

Answer:
No!

THE STORED COMMUNICATIONS ACT (SCA)

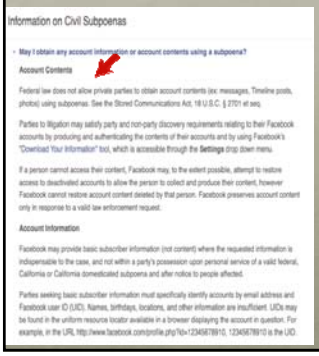
Why not!?

Because the SCA governs the disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs).

The Problem:

- The SCA was enacted ***in 1986*** as Title II of the Electronic Communications Privacy Act ("ECPA").
- While technology has advanced dramatically since 1986, the statute has not undergone a significant revision since enacted in 1986– "eons ago in internet time."

SOCIAL MEDIA SUBPOENAS


Information on Civil Subpoenas

- May I obtain any account information or account contents using a subpoena?

Account Contents

Federal law does not allow private parties to obtain account contents (ex: messages, Timeline posts, photos) using subpoenas. See the Stored Communications Act, 18 U.S.C. § 2701 et seq.

Parties to litigation may satisfy party and non-party discovery requirements relating to their Facebook accounts by producing and authenticating the contents of their accounts and by using Facebook's "Download Your Information" tool, which is accessible through the Settings drop down menu.

If a person cannot access their content, Facebook may, to the extent possible, attempt to restore access to deactivated accounts to allow the person to collect and produce their content, however Facebook cannot restore account content deleted by that person. Facebook preserves account content only in response to a valid law enforcement request.

Account Information

Facebook may provide basic subscriber information (not content) where the requested information is indispensable to the case, and not within a party's possession upon personal service of a valid federal, California or California domesticated subpoena and after notice to people affected.

Parties seeking basic subscriber information must specifically identify accounts by email address and Facebook user ID (UID). Names, birthdays, locations, and other information are insufficient. UIDs may be found in the uniform resource locator available in a browser displaying the account in question. For example, in the URL http://www.facebook.com/profile.php?id=1234567890, 1234567890 is the UID.

- Virtually every provider you attempt to subpoena will refuse to comply citing the Stored Communication's Act (18 U.S.C. § 2701) as its defense.
- Providers will assert the SCA prohibits them from "disclosing the contents of an account to any non-governmental entity pursuant to a subpoena or court order."

C. RULE 34 DISCOVERY REQUEST

So, how do we get this information?

1. Request download of all content;
2. Request a "Release" or "Authorization" from the user to obtain the content directly from the provider;
3. Request the user's Password; or
4. Request a Forensic Image of the content.

C. RULE 34 DISCOVERY REQUEST

1. Request download of all content.

- **Facebook.** Allows users to "***Download Your Info***." A zip file, for example, may be created which contain all of the user's content including messages, photos, posts and related information.
- **Google**. Allows users through "***Google Takeout***" to similarly download their content for production.
- **Twitter.** Allows a user to download all tweets by requesting a copy of the user's "***Twitter Archive***."
- **Third-Parties Services**, which archive and collect social media, including CloudPreservation and X1 Social Discovery, are available.

C. RULE 34 DISCOVERY REQUEST

2. Request a "Release" or "Authorization" from the user to obtain the content directly from the provider.

- Many providers have a form to be used.

C. RULE 34 DISCOVERY REQUEST

3. Request the user's Password.

- This idea seems fraught with peril for both sides as the "obtainer" of the password could make changes, send messages, go into the user's "Friends" accounts and the like,
- *or* the "user" could claim they did not produce the content.

C. RULE 34 DISCOVERY REQUEST

4. Request a Forensic Image of the content.

- Because of evidentiary chain of custody issues, this is best done by a professional third-party.

V. CAN WE RECOVER DELETED OF LOST INFORMATION?

Answer: We need an Expert.

- Is the Juice Worth the Squeeze?

Data Locations

• Desktop and laptop computers	• Servers (file, internet, email)
• External hard drives	• Backup tapes
• Cell phones / Smart phones	• iPads / Tablets
• Flash drives	• Floppy disks
• CDs / DVDs	• Home systems

Types of ESI

• Email	• Office docs / PDFs
• Databases	• Internet history
• Calendars	• Accounting records
• Social Media	• IM logs
• Newsgroups	• System history files
• Cache files	• Cookies
• Blogs	• Digital voice mail

Deleted versions of all of the above!

"On the Internet, nobody knows you're a dog."

What Happens When I Hit the "Delete" Key?

- Think of the computer as a library and a card catalog where books in the library represent data files on the computer.
- The computer keeps an index of all the active files on a computer … the cards in the card catalog. When a file is deleted, the "book" is not pulled from the shelf. The card is simply removed from the card catalog and the spot on the shelf is listed as being "available".
- When the system needs space for a new file, that same shelf spot may be chosen, but most likely it will not be. The un-cataloged book may sit on the shelf for a day or for years.
- Think It's Deleted? … Think Again!

Secure the Image: Act Fast

- It's all about preservation.
- Deleted data can be overwritten at any time.
- Every time a computer is turned on, latent data gets overwritten.
- Once latent data is overwritten, it's pretty much gone forever.
- Only forensic images preserve the status quo and preserve latent data.

Secure the Image: Easy Parts First – Hard Parts Later

- Forensic investigators need not view the contents of a hard drive when creating an image, so arguments of relevance, privilege, and admissibility can be saved for another day.
- Opposing counsel and judges don't understand this – educate them!
- The minimal expense of securing forensic images early can make the difference between winning and losing a case.

"O.K., you've just sentenced him to twenty-five years to life—now push 'send.'"

Secure the Image

Your IT People Can't Do This!

- Common litigation mistake is entrusting collection and preservation of ESI to the client or law firm's IT people.
- Although skilled at what they do, IT people are not forensically trained, certified, and normally do not have the proper court-accepted tools.
- Without training, certification, and experience, you can fail to find something important or render what you do find inadmissible in court.
- The courts require that you use qualified personnel.

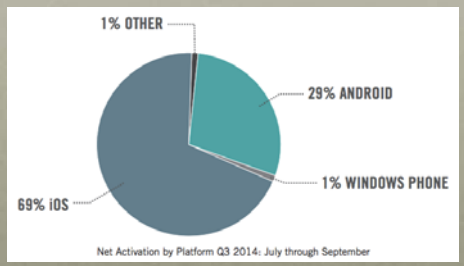
Secure the Image: Don't Cut Corners

- Don't Cut Corners by using slipshod procedures or unqualified personnel to perform work that may be offered in court.
- Trained and certified computer forensic investigators never:
  - Boot from the original hard drive
  - Connects original hard drive without using hardware write protection
  - Take a "quick peek" at the data
  - Use the original media in the analysis
  - Use software that is non-court-approved or unlicensed
- Never!

Mobile Device Challenges

- Unlike the computer realm's limited number of vendors, there are countless manufacturers of mobile devices.
- Each mobile device manufacturer uses one of many proprietary file systems and formats.
- Growth and development in the mobile device world is fast. Updates and changes are released almost weekly.
- Not all devices supported.

Market Share

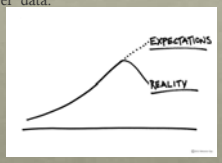


Mobile Device Forensic Tools

- Cellebrite
- Oxygen Suite
- MPE, AccessData
- Paraben
- IEF
- DD Commands

When Dealing with Law Enforcement…

- Cellebrite reports are commonly provided. These contain what the police choose to include.
- When possible, request the forensic image or extraction.
- Further analysis can be conducted on the image/extraction to discover/recover data.



Types of ESI on Mobile Devices

• Email	• Application Data
• Call Logs	• Internet history and cookies
• Calendars	• Documents
• Text Messages	• Wi-Fi History
• Photos	• Contacts
• Location Data	• Sync Logs
• Videos	• Voice mail

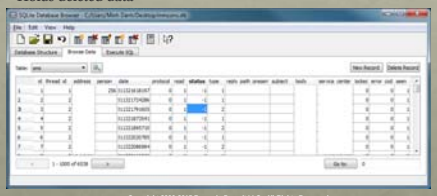
Deleted versions of many of the above!

Deleted Data

- Deleted text messages, call logs, browsing history and more exists inside SQLite databases.
- Deleted pictures can leave behind thumbnails.
- Deleted videos, pictures, and documents can often be recovered from SD cards

SQLite Databases

- A file system within a file system…almost
- Manages data for applications
- Holds deleted data



Device Modification

- Rooting and Jailbreaking are both used to gain admin or root level access to a device.
- Once root access is obtained, databases that were once inaccessible are usually able to be extracted and parsed.
- Last Resort!

Android: Super User

Apple iOS: Cydia

JTAG: Joint Test Action Group

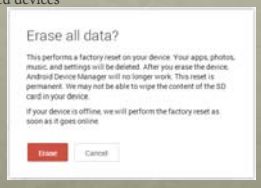
- Locked proprietary OS phones
- Physical acquisition
- Damaged or broken phones
- Unsupported by forensic tools
- Password protected devices

Chip-Off

- Last and most intrusive method to get a physical image
- Desolder the NAND chip and connect it to a memory chip
- Potential danger of total data destruction

Remote Wiping

- Both Android and Apple iOS devices can be remotely wiped
- Email and password required
- Difficult to recover data from wiped devices



Remote Wiping

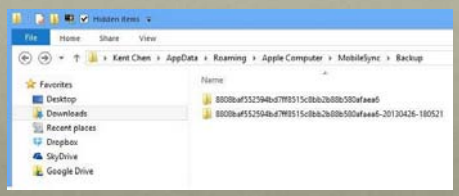
- Use a Faraday Bag to prevent wireless signals from communicating with the device.
- Turn on airplane mode
- Never power on a phone outside of a Faraday bag. Wipe commands are received during boot.

Syncing and Backups

- Almost all data can be stored on the cloud or locally.
- Many options available: Google, iCloud, OneDrive, etc.
- Deleted content on one device can be found alive and well on another.
- Users are not always aware backups exist!
- Full restores of phones possible by using backups from iTunes.

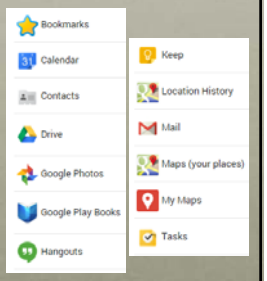
Apple iOS Backups

- iTune backups contain SQLite databases that hold deleted data
- iCloud backups hold similar data but require an email and password



Google Account Backups

- Gmail and password required
- Available for Android devices and Google Accounts
- Deleted data not included
- Not as rich as Apple backups



Bypassing Lock Codes

- Lock codes can sometimes be bypassed. This varies by model.
- iPhone security on older model iPhones can be circumvented by using data from a computer it has synced with in the past or using specialized tools.
- Android devices can be modified to extract data.

Damaged Devices

- Data can be recovered from broken devices in most situations.
- More often than not, data is intact.
- Water damaged phones can sometimes be salvaged.
- Chip-offs and J-Tagging.

VI. JUDICIAL REMEDIES

VI. JUDICIAL REMEDIES

The Challenge:

- **How do you *quantify* the sanctions you are asking for?**
  - **Especially, if you don't know what has been deleted, only that spoliation has occurred?**
- Very difficult for judges to make ***commensurate sanctions***. Depends on the facts of each case.

VI. JUDICIAL REMEDIES

Most courts will treat spoliation as a form of discovery abuse, sanctionable pursuant to C.R.C.P. 37.

What Remedies are available in Family Law?

- A. Attorney fees and costs incurred due to spoliation;
- B. "Adverse Inference" as to the spoliated evidence;
- C. Preclusion of certain testimony;
- D. Monetary Sanction (against the party or counsel);
- E. Creative remedies to the action.

QUESTIONS?