

Stange Law Firm P.C.

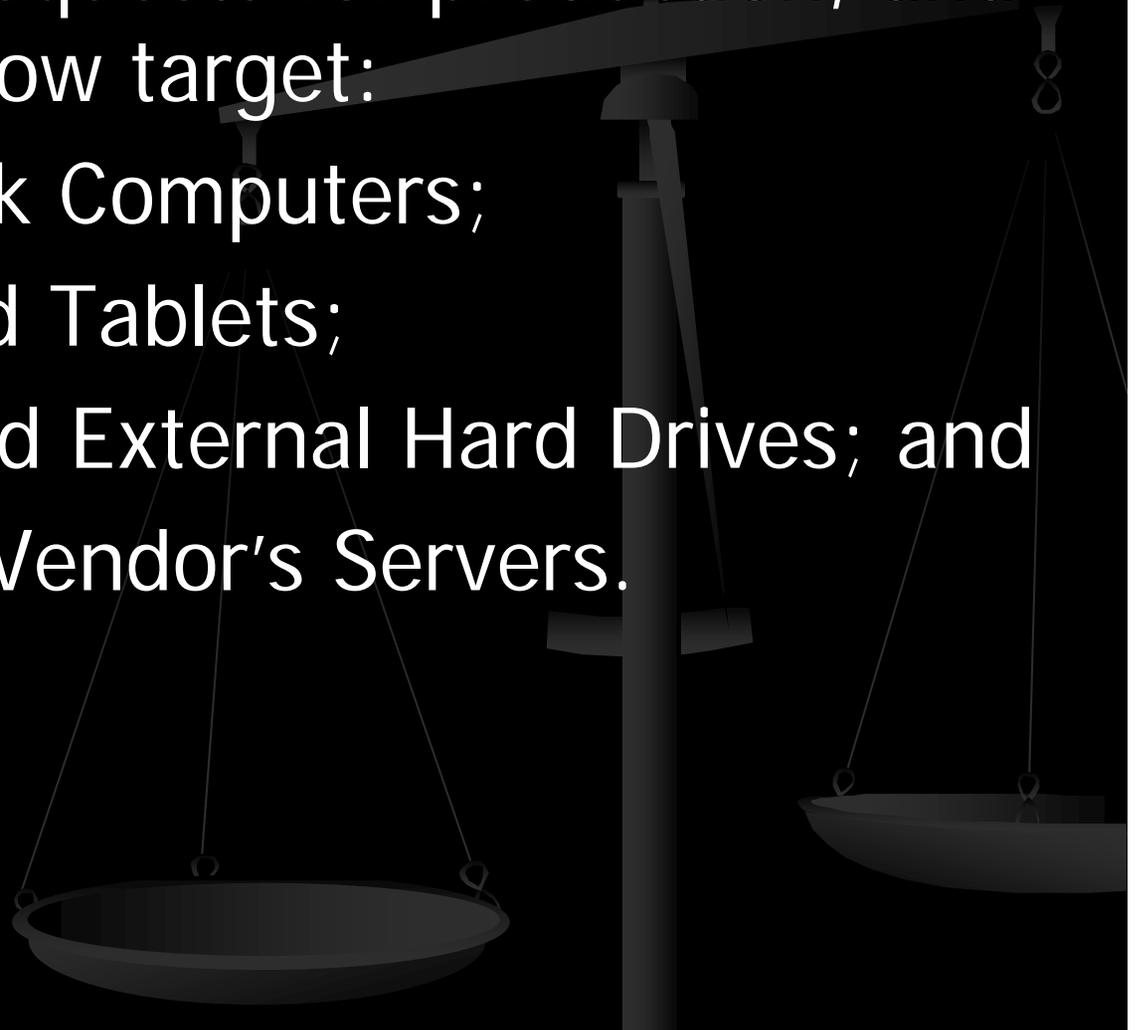
Smart Phone & Social Media
Evidence For Lawyers &
Judges

Kirk C. Stange, Esq.



New Sources for Traditional Discovery Tools

- Interrogatories, requests for production, and depositions can now target:
 - Home and Work Computers;
 - Cell Phones and Tablets;
 - Flash Drives and External Hard Drives; and
 - Cloud Storage/Vendor's Servers.



Home and Work Computers

- 18 U.S.C. § 1030 or the Computer Fraud and Abuse Statute is the overarching Federal Statute on point
 - (a) intentionally accessing a computer without authorization from any protected computer if the conduct involved an interstate or foreign communication;
 - (b) knowingly and with intent to defraud, accessing a protected computer without authorization, or exceeding authorized access, and by means of such conduct furthering the intended fraud; and
 - (c) intentionally accessing a protected computer without authorization, and as a result of such conduct, causing damage.



Home and Work Computers

- State Courts have been all over the place on the balance between privacy and discoverability
 - *Rosenberg v. Rosenberg*, No. C4-01-1148, 2002 WL 15649 (Minn. Ct. App. Jan. 8, 2002).
 - Wife believed there could be evidence on the husband's computer of hidden assets, but otherwise, she had no real evidence of concealment. The court found the wife's requests for authorizations to access the husband's business computer to be invasive and based purely on conjecture. Thus, the appellate court upheld the denial of the discovery requests.
 - *Byrne v. Byrne*, 650 N.Y.S.2d 499 (N.Y. Sup. Ct. 1996).
 - Husband's laptop computer was owned by his employer, but was also used for his personal finances unrelated to his employment. The wife had her lawyer copy the computer's memory. The court concluded that the computer, commonly located in the marital home, was akin to a file cabinet within the marital home. Clearly, the wife could have access to the contents of each.

Home and Work Computers

- *Stafford v. Stafford*, 641 A.2d 348 (Vt. 1993).
 - Wife found a file on the family computer called "My List," which was similar to a notebook she had found detailing husband's sexual encounters with various women. The notebook disappeared before trial, but the court found the file on the family computer to be sufficient to identify the notebook for what it was, which was a list of adulterous encounters.
- *State v. Appleby*, 2002 WL 1613716 (Del. Super. Ct. July 18, 2002).
 - Husband and wife routinely commingled computer hardware. Despite wife having possession at time of trial, it was "theirs" in every sense.

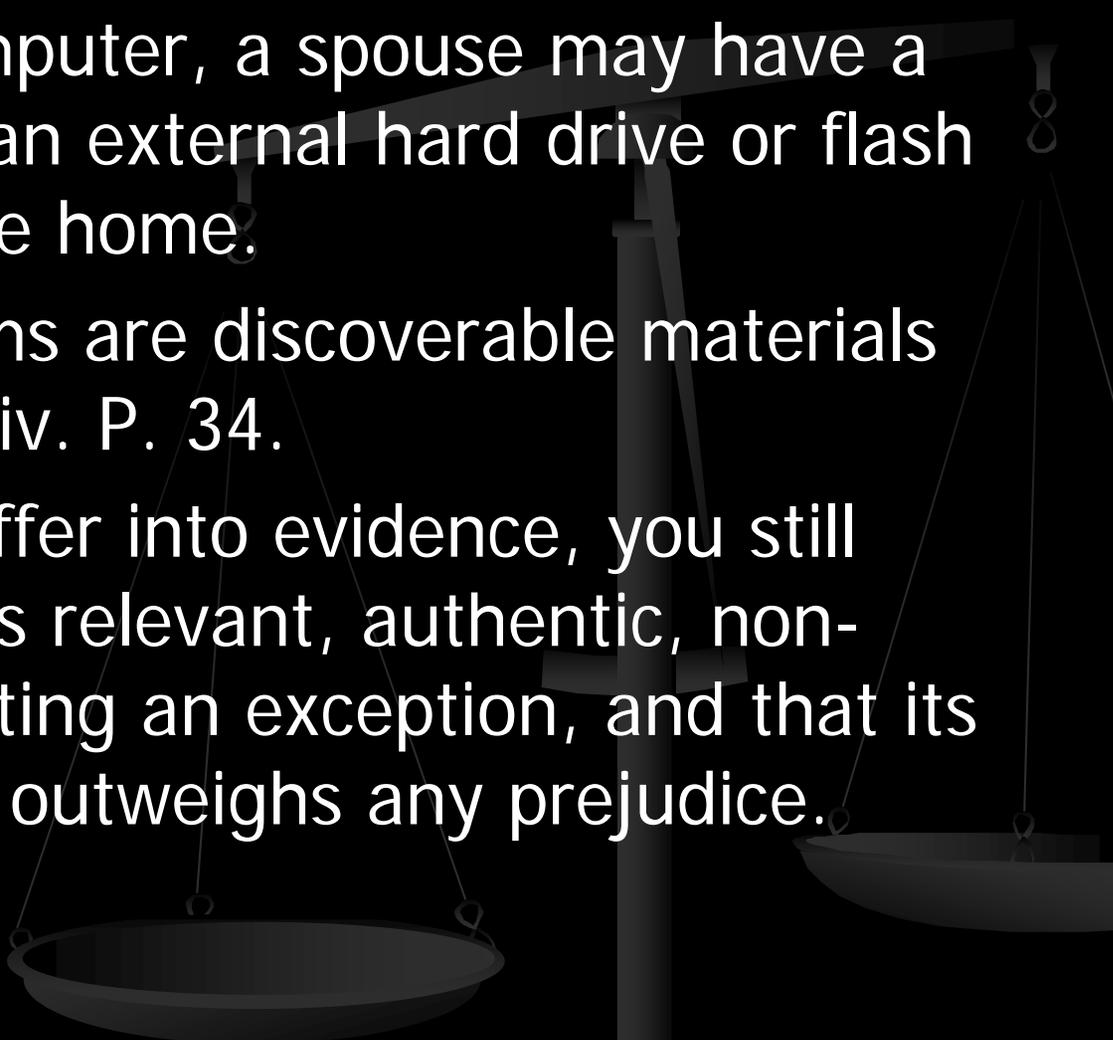
Smart Phones and Tablets

- In the realm of cell phones and tablets lurk two significant federal statutes: Title III of the Omnibus Crime Control Act 1968-2522 and Electronic Communications Privacy Act of 1986.
- Together, they prohibit interception of oral and electronic communication without consent of at least one party to the communication.
- These apply to traditional telephones, wireless phones, and cell phones.
- As a practical note, secretly recorded oral communications are almost always excluded at trial, whereas electronic communications are almost never automatically excluded.
- For example, in *Conner v. Tate*, a woman had a cause of action against her lover's wife who was intercepting phone conversations and recording voicemail messages. 130 F. Supp. 2d 1370 (N.D. Ga. 2001).

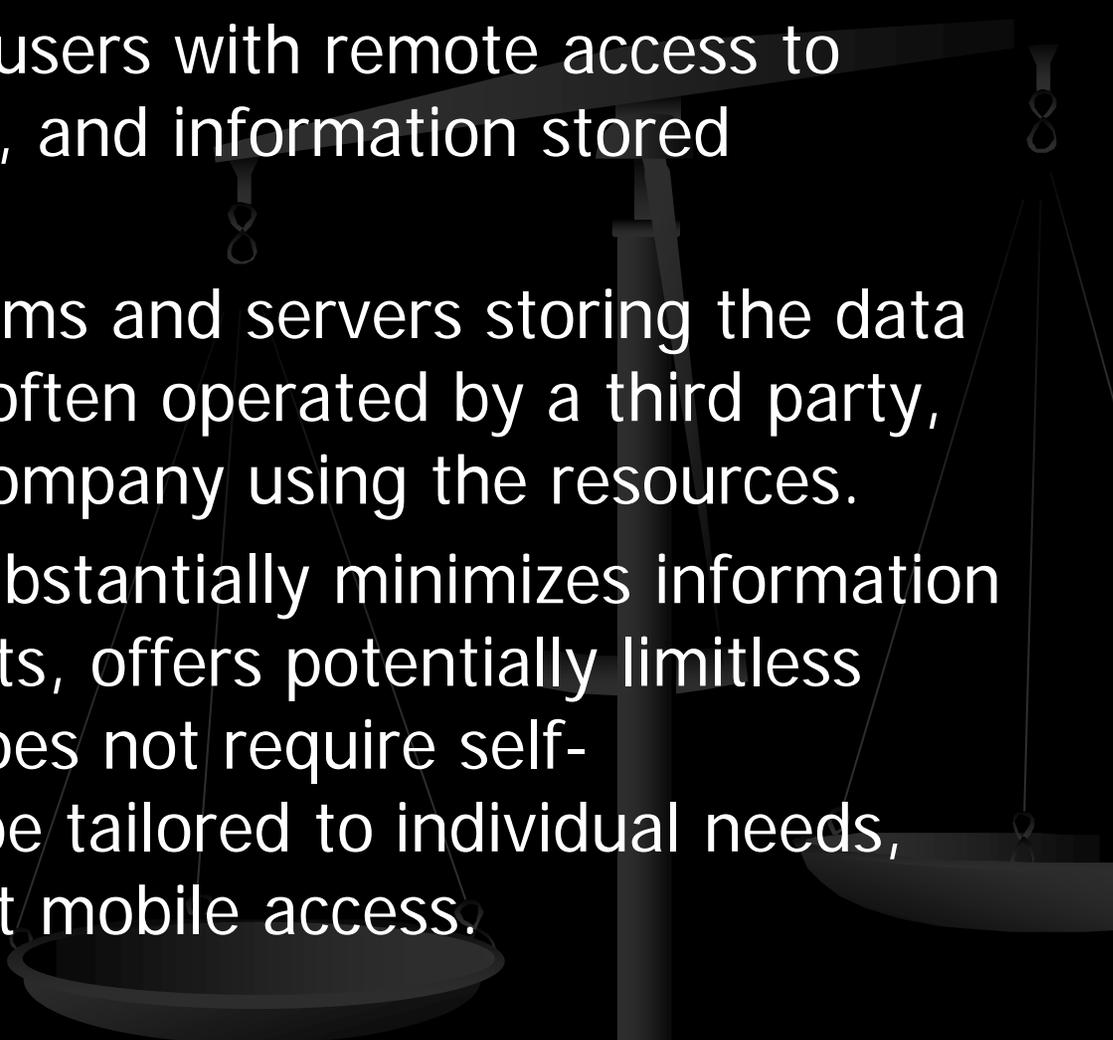
Flash Drives and External Hard Drives

- Knowing the technology can be crucial in E-discovery, so that you know what and how to retrieve data.
- Both flash drives and external hard drives are back-up storage mechanisms for a user's computer.
- Generally, each may be used to store all of the types of data found on a traditional computer or internal hard drive, including word processor documents, spreadsheets, photos, and videos.

Flash Drives and External Hard Drives

- Similar to a computer, a spouse may have a right access to an external hard drive or flash drive used in the home.
 - If not, such items are discoverable materials under Fed. R. Civ. P. 34.
 - If planning to offer into evidence, you still must ensure it is relevant, authentic, non-hearsay or meeting an exception, and that its probative value outweighs any prejudice.
- 

Cloud Storage

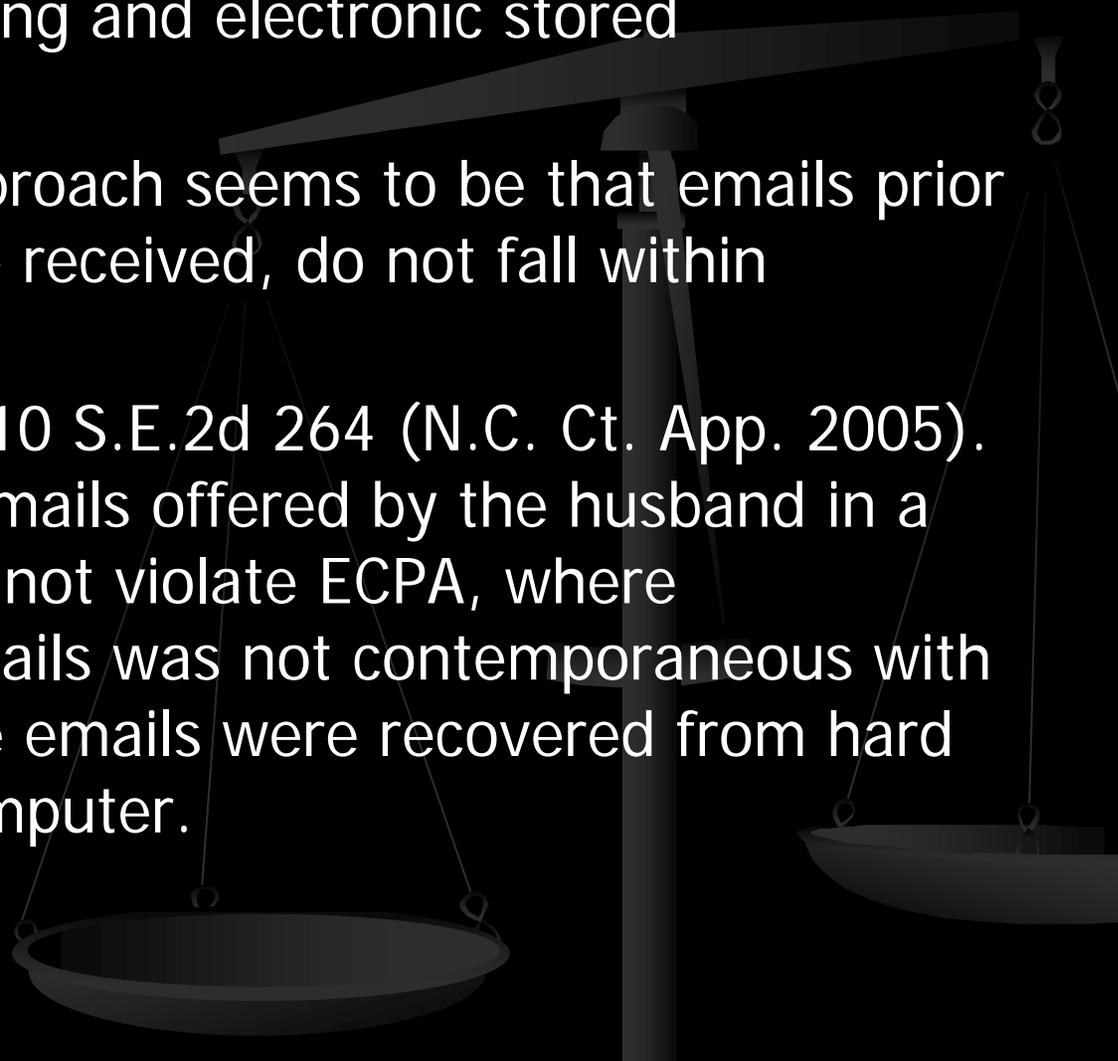
- Essentially, the cloud allows for internet based services to provide users with remote access to software, resources, and information stored elsewhere.
 - The computer systems and servers storing the data or applications are often operated by a third party, not the person or company using the resources.
 - Cloud computing substantially minimizes information technology (IT) costs, offers potentially limitless storage capacity, does not require self-management, can be tailored to individual needs, and provides instant mobile access.
- 

Cloud Computing

- Having a basic knowledge of your provider will help you:
 - Negotiate the service agreement to begin with;
 - Locate data when litigation arises; and
 - Ensure that the data is unaltered when it comes time to produce.
- These may be particularly important because Fed. R. Civ. P. 34(a) which defines discoverable information as “in the responding party’s possession, custody, or control.”
- Federal courts have held that data in the possession of a third party to be within Rule 34(a) so long as the party “has the right, authority, or practical ability to obtain the documents from a non-party to the action. *Goodman v. Praxair Services, Inc.*, 632 F. Supp.2d 494 (D. Md. 2009).
- Third party control through a cloud may leave the user subject to sanctions when the data has been moved, altered, or is otherwise inaccessible.

Types of Data: Emails

- The use of email by opposing spouses falls within the interplay of wiretapping and electronic stored communications.
- The predominant approach seems to be that emails prior to being sent or once received, do not fall within wiretapping statute.
 - *Evans v. Evans*, 610 S.E.2d 264 (N.C. Ct. App. 2005). Sexually explicit emails offered by the husband in a divorce action did not violate ECPA, where interception of emails was not contemporaneous with transmission. The emails were recovered from hard drive of family computer.



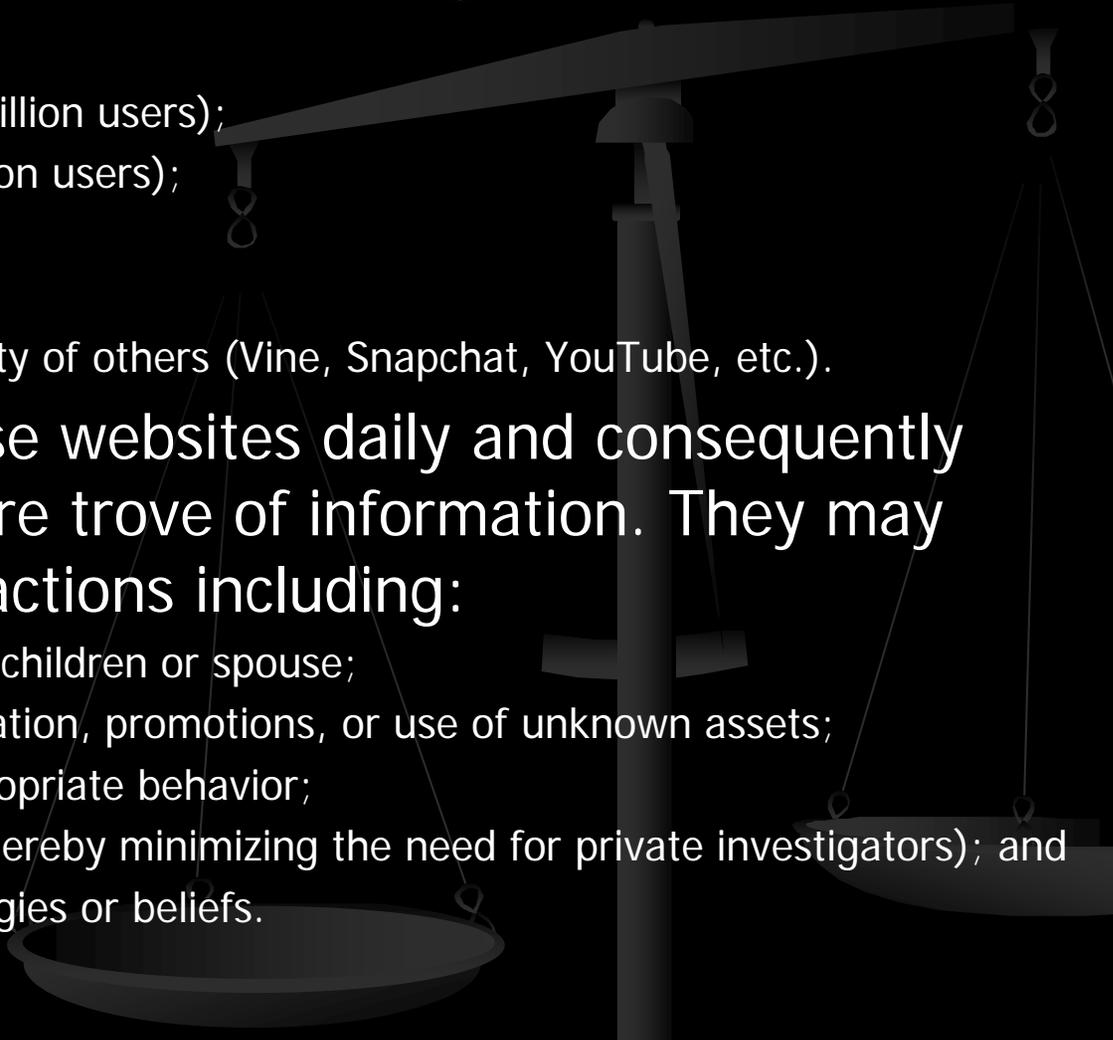
Types of Data: Emails

- *O'Brien v. O'Brien*, 899 So.2d 1133, 1138 (Fla. Dist. Ct. App. 2005). Court concluded that spyware capturing emails in a family law case did violate ECPA and admission of these emails was within discretion of trial court.
- *White v. White*, 781 A.2d 85 (N.J. Super. Ch. 2001). Wife hired a computer expert to find and copy her husband's emails that were stored on the hard drive of the computer in the family home.
 - Wife did not violate the SCA because the email was not in electronic storage when it was accessed.
 - It was also determined that the access was not without authorization.

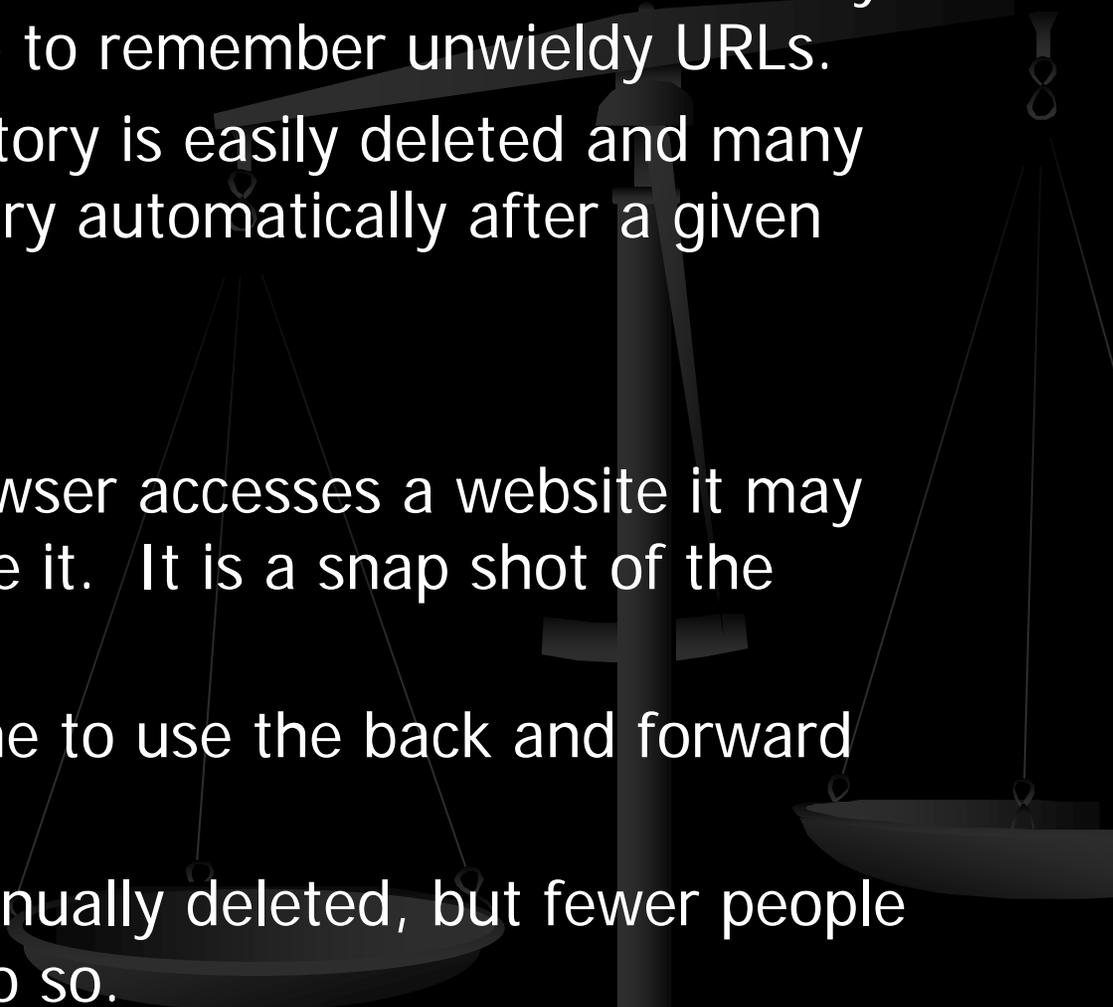
Types of Data: Cell Phones and Text Messages

- The most common application for cell phones is to subpoena the carrier for itemized billing, but that is changing.
- Text messages or Short Message Service (SMS) messages may be worth tracking down because a lot may be said in the 224 characters that some phones now allow.
- SMS messages may also transmit photos, sounds, and videos.
- Retrieving this source of data quickly, can be vital because most carriers routinely delete text messages within a day or two.
- However, forensic experts can often pull deleted text messages sent or received long ago from the device itself.
- Outside of intercepting telephone conversations or voicemails, smart phone data and tablets are akin to a computer.

Types of Data: Social Media

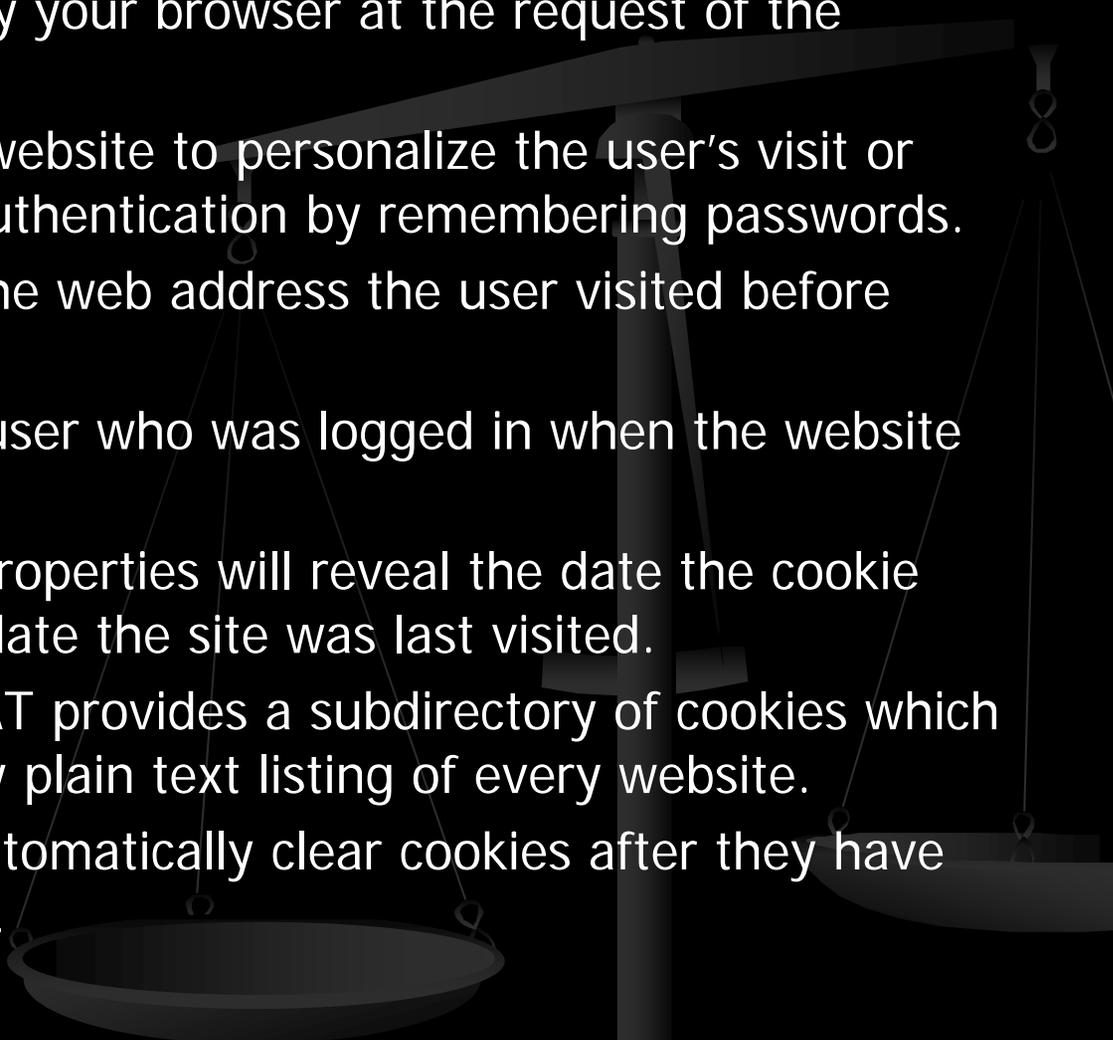
- There are numerous social networking sites out there including:
 - Facebook (over 750 million users);
 - Twitter (over 200 million users);
 - Google Plus;
 - Linked-In;
 - My Space; and a variety of others (Vine, Snapchat, YouTube, etc.).
 - People often use these websites daily and consequently they contain a treasure trove of information. They may reveal a time line of actions including:
 - time spent away from children or spouse;
 - boastings of compensation, promotions, or use of unknown assets;
 - photographs of inappropriate behavior;
 - potential witnesses (thereby minimizing the need for private investigators); and
 - and/or extreme ideologies or beliefs.
- 

Types of Data: Browser History

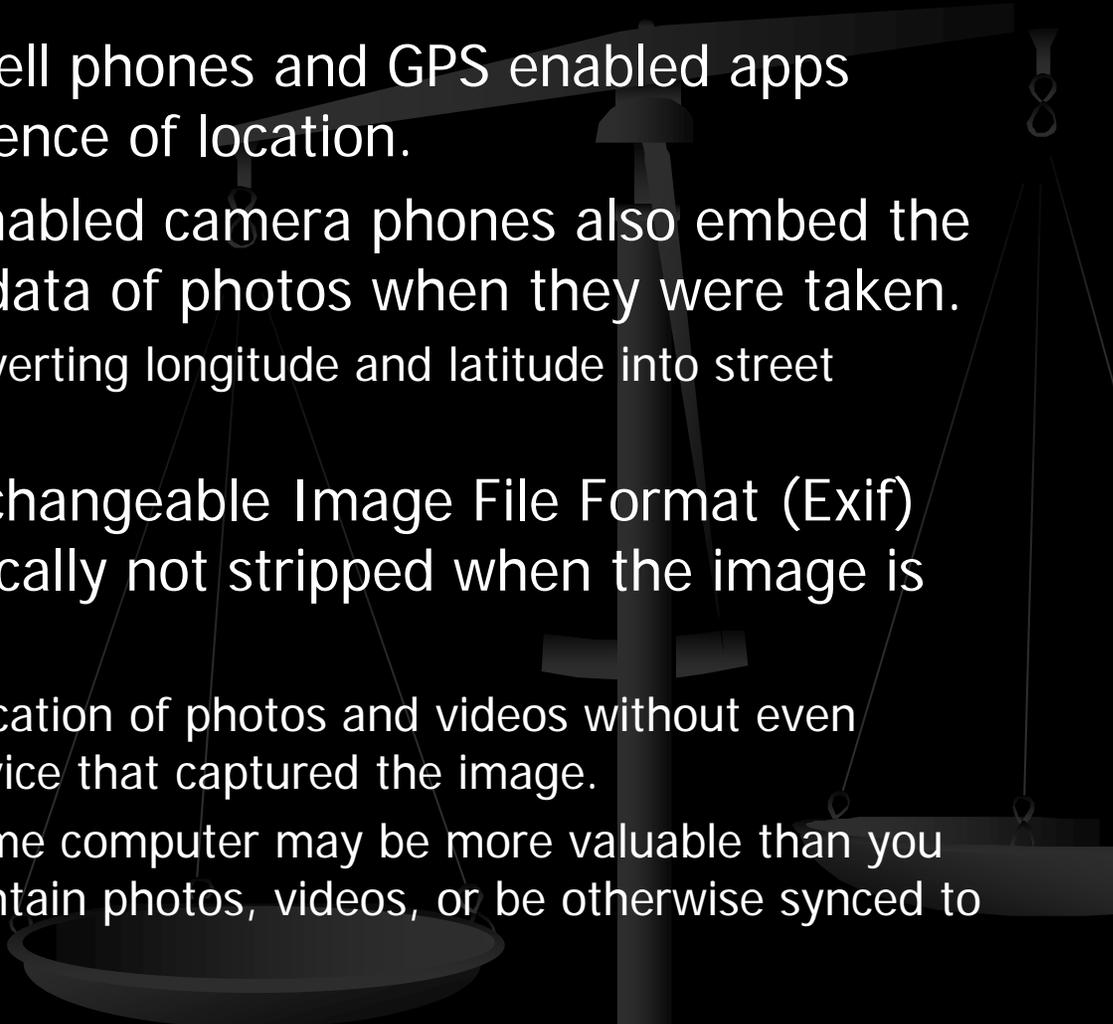
- Browser History:
 - Most are aware that browsers track our history so we do not have to remember unwieldy URLs.
 - A browser's history is easily deleted and many delete the history automatically after a given period of time.
 - Cached Files:
 - When your browser accesses a website it may cache it or store it. It is a snap shot of the webpage.
 - This enables one to use the back and forward tabs.
 - Can also be manually deleted, but fewer people remember to do so.
- 

Types of Data: Browser History

■ Cookies:

- Cookies are created by your browser at the request of the website.
 - These files allow the website to personalize the user's visit or speed up the user's authentication by remembering passwords.
 - Cookies can contain the web address the user visited before entering its website.
 - They may reveal the user who was logged in when the website was accessed.
 - Clicking on the file's properties will reveal the date the cookie was created and the date the site was last visited.
 - A file called INDEX.DAT provides a subdirectory of cookies which lists at least a partially plain text listing of every website.
 - Many browsers will automatically clear cookies after they have reached a certain age.
- 

Types of Data: Geolocation Data

- Cell towers, GPS, and WiFi all serve to create geolocation data.
 - The data provided by cell phones and GPS enabled apps provides objective evidence of location.
 - Moreover, most GPS enabled camera phones also embed the longitude and latitude data of photos when they were taken.
 - Many apps exist for converting longitude and latitude into street addresses.
 - This data known as Exchangeable Image File Format (Exif) metadata, and it is typically not stripped when the image is emailed or uploaded.
 - This allows for the verification of photos and videos without even having access to the device that captured the image.
 - And, it means that a home computer may be more valuable than you think because it may contain photos, videos, or be otherwise synced to a mobile device.
- 

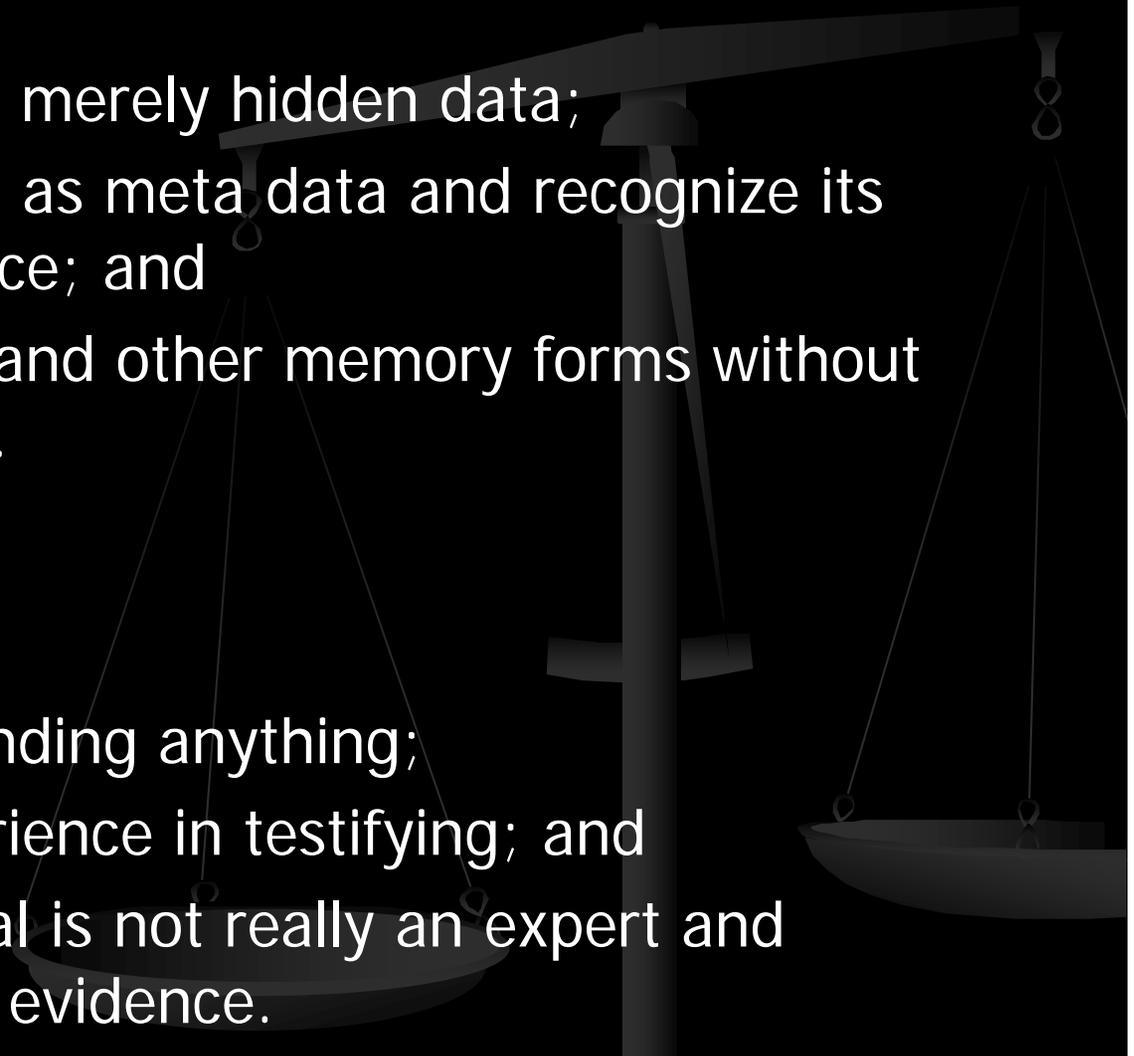
Pros and Cons of Using Outside Investigators

■ Pros:

- Recover deleted or merely hidden data;
- Discover data such as meta data and recognize its potential significance; and
- Mirror hard drives and other memory forms without damaging the files.

■ Cons:

- Expensive;
- No guarantee of finding anything;
- May have no experience in testifying; and
- Possibility individual is not really an expert and damages potential evidence.



Case Law Update

- *In re Marriage of Bates*, 817 N.W.2d 32 (Iowa Ct. App. 2012).
 - The court cited an email from the wife to the husband saying, "You will never feel so much pain when I'm done with you...I'm going to embarrass [sic], you make the kids hate you."
 - This supported an evaluator's finding of alienation and the court upheld an award of sole legal custody to the father.
 - For the purposes of awarding sole physical custody, mother's posts on Facebook stating that the children "have a really bad father" were relevant as oldest child could clearly access Facebook.
- *Safdar v. AFW, Inc.*, 279 F.R.D. 426, 430 n. 41 (S.D. Tex. 2012).
 - Plaintiff filed suit against former employer under the FLSA.
 - Plaintiff used printouts from defendant's Facebook page to corroborate his story regarding the size of defendant's business.
 - The defendant's Facebook page listed nine stores, the same number cited in the plaintiff's affidavit, whereas the defendant had claimed just two stores in his own affidavit.

Case Law Update

- *Leenhouts v. Leenhouts*, No. M2012-01844-COA-R3-CV, 2013 WL 3968159, at *2-*4 (Tenn. Ct. App. July 31, 2013).
 - In a divorce action, wife placed a motion for default on husband's desk in marital home.
 - Husband, several days later, placed messages on Facebook to the tune of "you thought you had me" followed by several expletives.
 - While court was hesitant to use the post as proof of service, husband's testimony that he could not recall who his Facebook post was directed at damaged his credibility to extent that the court believed he had received service.
- *Garcia v. City of Laredo, Tex.*, 702 F.3d 788 (5th Cir. 2012):
 - The Fifth Circuit affirmed the district court's interpretation of the Stored Communications Act ("SCA") and concluded that it does not apply to data stored in a personal cell phone. These were text messages and photographs.

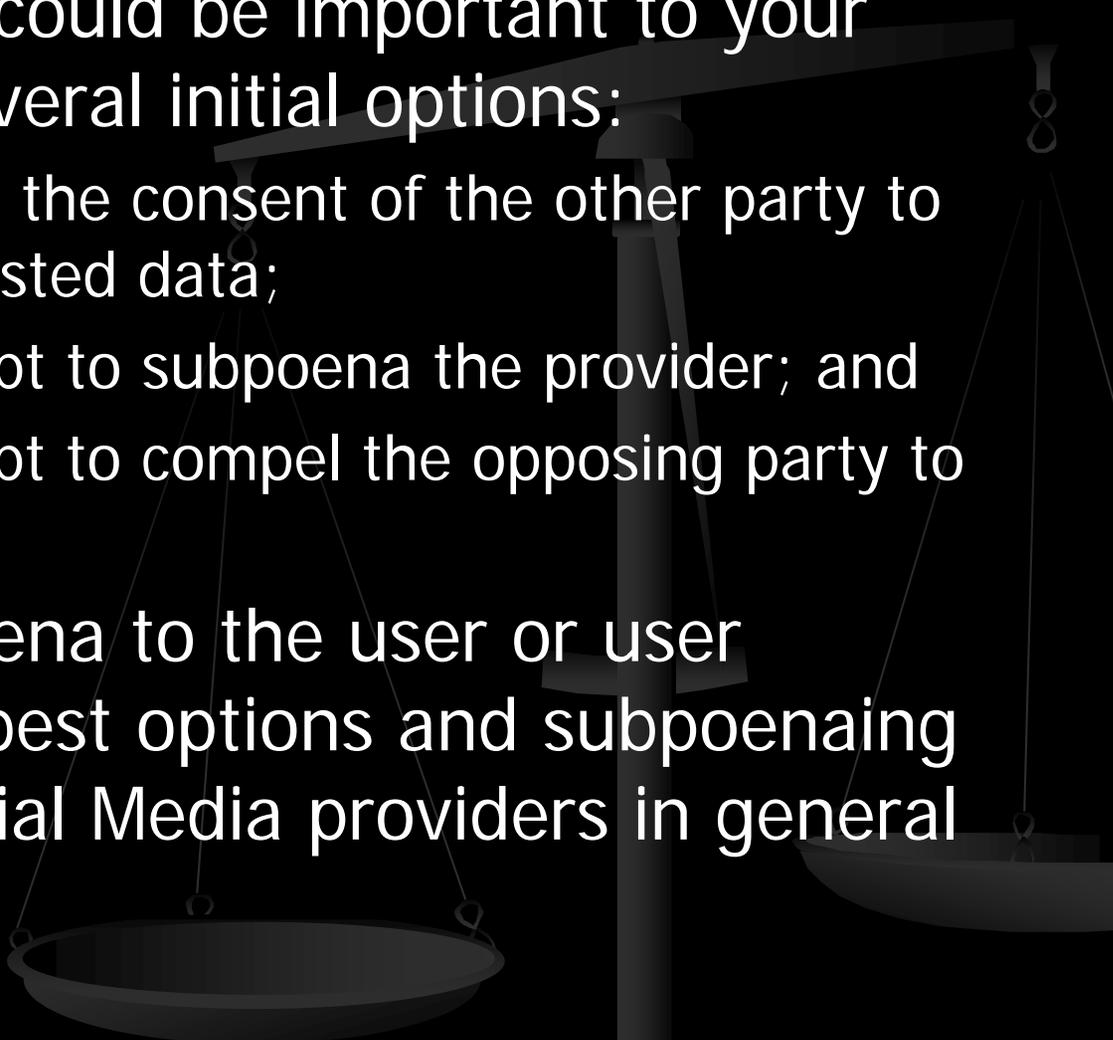
Case Law Update

- *Lazette v. Kulmatycki*, No. 3:12CV2416 2013, WL 2455937 (N.D. Ohio June 5, 2013).
 - In this case, the plaintiff's supervisor proceeded to read previously read personal, but not deleted emails on a former employee's blackberry.
 - The employee thought the device had been cleansed of personal communications, but still did not have an action under the SCA as to opened, but not deleted e-mailed, because it was the server that was the protected storage device, not the smart phone.
- *United States v. Walker*, 771 F. Supp. 2d 803, 810–11 (W.D. Mich. 2011):
 - The court found the attachment of a GPS device to the bumper of the defendant's car to be no more intrusive than "duct-taping an iPhone to Defendant's bumper."
 - The court seemed to reason that because so many people now carry GPS enabled phones, they cannot reasonably expect privacy as to their location.
 - In civil litigation it is even less likely for location data to be problematic as the 4th amendment applies to government action, not private.

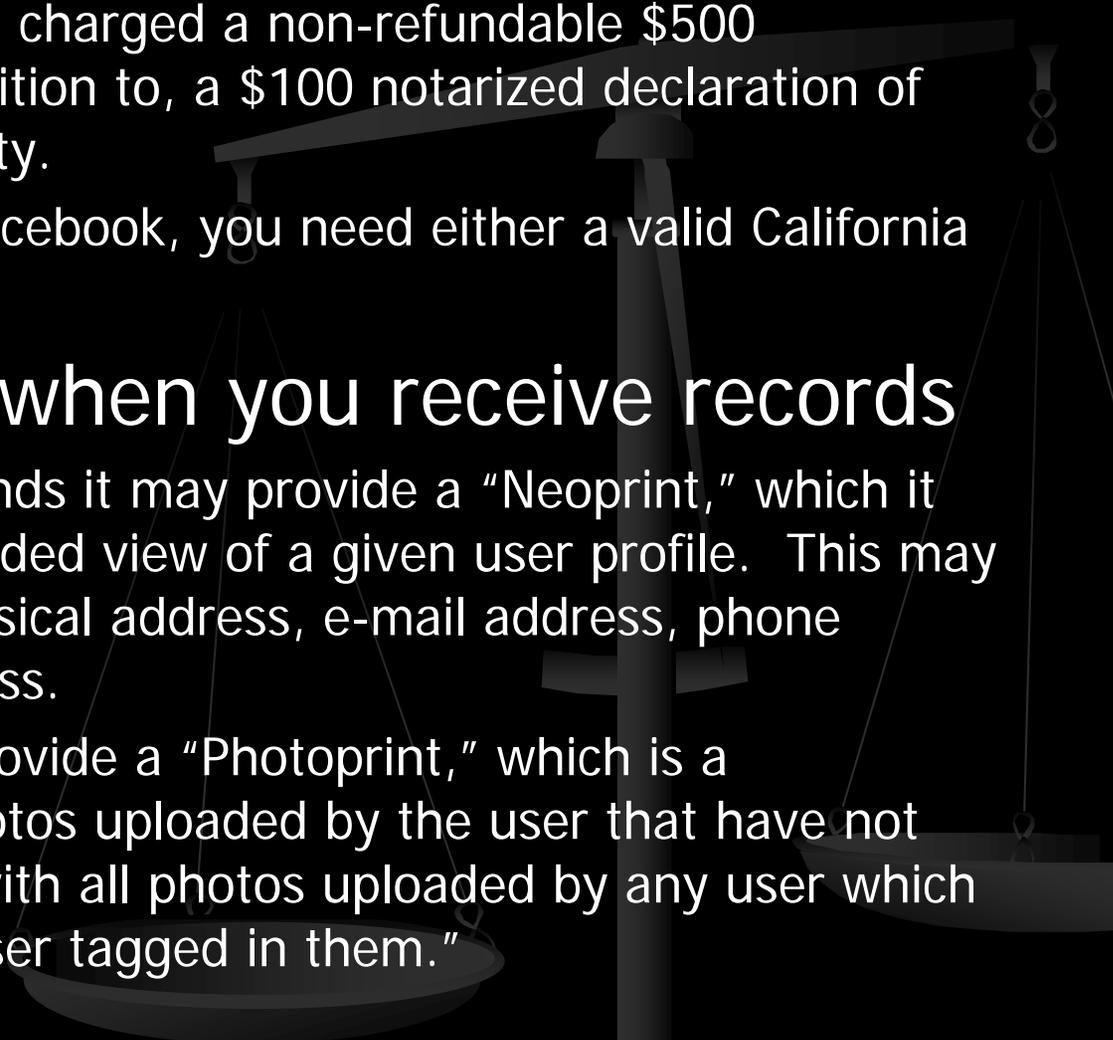
Case Law Update

- *Flagg v. City of Detroit*, 25 F.R.D. 346 (E.D. Mich. 2008).
 - A minor child, through his next friend, sued the mayor of Detroit alleging an inadequate investigation of the mother's death.
 - The plaintiff discovered that some four years after the incident, the wireless carrier, SkyTel, still had messages about the shooting that he believed might be relevant to the case.
 - The court ordered SkyTel to produce the text messages. *Id.* at 357. Also shows that sometimes carriers retain text data.
- *PTSI Inc., v. Haley*, No. 684 WDA 2012, 2013 WL 2285109, at *15 (Pa. Super. Ct. May, 24 2013).
 - The record was clear that the party routinely deleted messages due to volume of conversations to ensure that the party could still utilize the messaging function of the phone.
 - The appellate court was suspicious of the deletion of emails, but it would not hold the trial court abused its discretion in choosing not to award sanctions.

Facebook Discovery

- Once you have decided that social media content will be or could be important to your case, you have several initial options:
 - (1) you can obtain the consent of the other party to produce the requested data;
 - (2) you can attempt to subpoena the provider; and
 - (3) you can attempt to compel the opposing party to produce the data.
 - Typically, a subpoena to the user or user consent are your best options and subpoenaing Facebook and Social Media providers in general can be difficult.
- 

Subpoenaing Facebook



- Subpoenaing Facebook is expensive
 - In the past, they have charged a non-refundable \$500 processing fee, in addition to, a \$100 notarized declaration of the records authenticity.
 - Also, in the case of Facebook, you need either a valid California or federal subpoena.
- What to expect when you receive records
 - If the company responds it may provide a "Neoprint," which it describes as an expanded view of a given user profile. This may include the user's physical address, e-mail address, phone number, and IP address.
 - Facebook also may provide a "Photoprint," which is a "compilation of all photos uploaded by the user that have not been deleted, along with all photos uploaded by any user which have the requested user tagged in them."

Subpoenaing Facebook: Difficulties Ahead

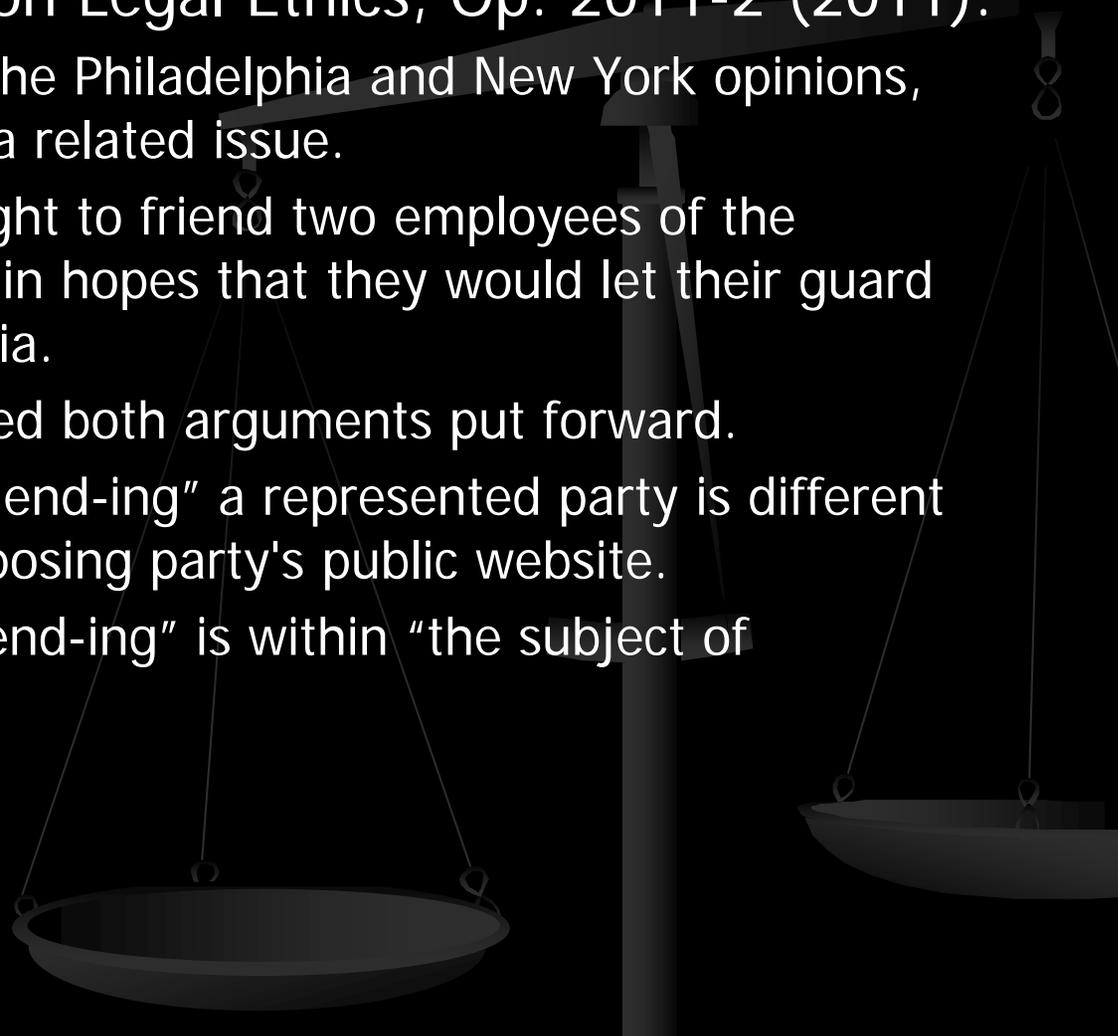
- In the wake of *Crispin* a case we will talk about later in the presentation, and the SCA, it appears unlikely that MySpace and Facebook would divulge private content subject to a civil subpoena without the user's consent.
 - In fact, Facebook's own policy seems to answer this question: "Federal law prohibits Facebook from disclosing user content (such as messages, Wall (timeline) posts, photos, etc.) in response to a civil subpoena." "Specifically, the Stored Communications Act, 18 U.S.C. §2701 et seq., prohibits Facebook from disclosing the contents of an account to any non-governmental entity pursuant to a subpoena or court order."

The Ethical Risks of Using “Friend-ing” to Obtain Personal Information

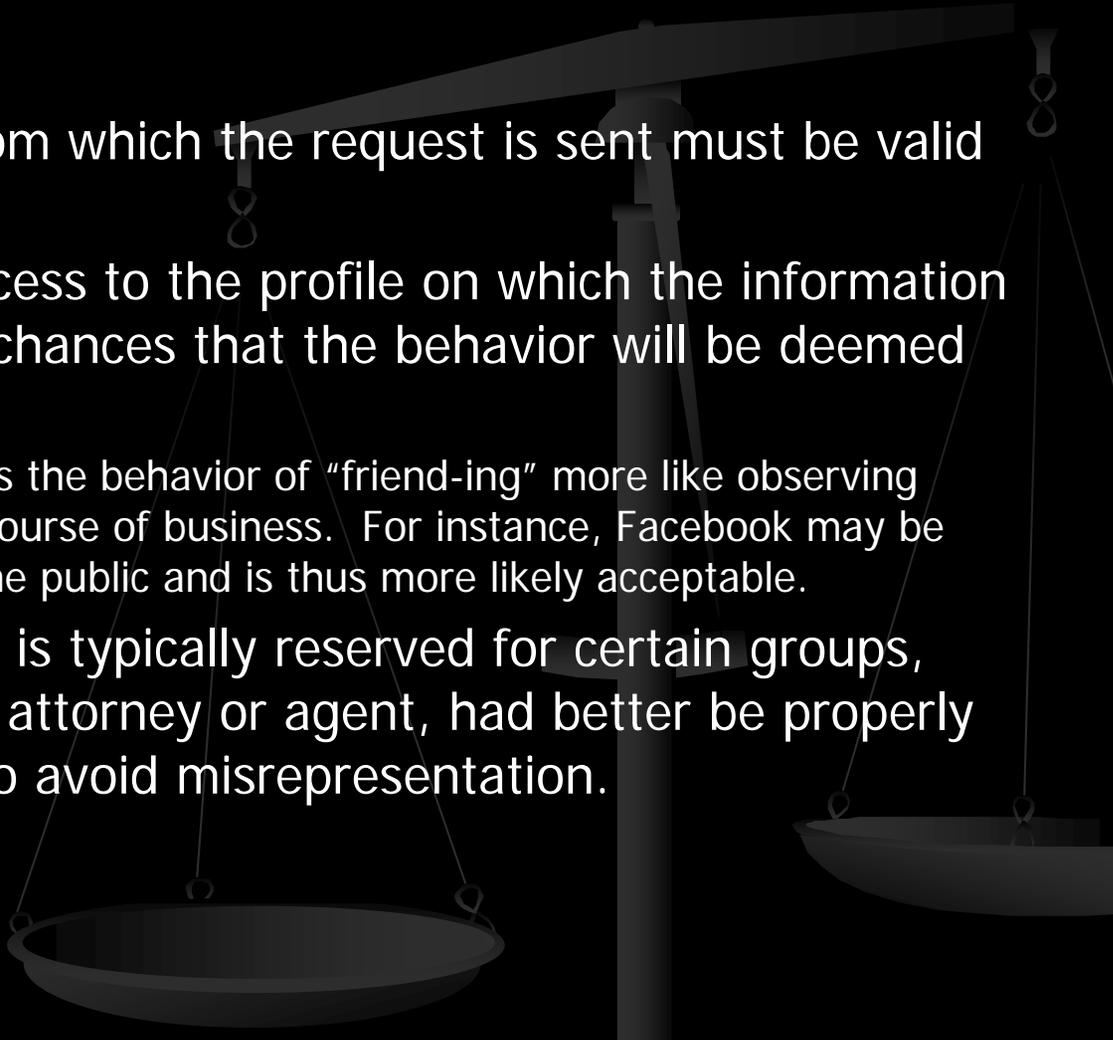
- Two bar opinions have addressed this issue reaching different results
 - Phila. Bar Ass'n Prof'l Guidance Comm., Op. 2009-02 (2009).
 - The Committee found an investigator, working for a lawyer, could not send a friend request to a hostile third party witness. The opinion concluded that this was deceptive, even though the investigator's profile contained accurate information. The act was deceptive because the investigator was omitting a highly material fact; that the purpose was to provide access to the attorney.
 - N.Y. City Bar Ass'n Comm. On Prof'l & Judicial Ethics, Formal Op. 2010-2 (2010).
 - Here, the committee found it was ethical for an attorney or agent of the attorney to “use her real name and profile to send a friend request to obtain information from an unrepresented person's profile.” The opinion did find an ethical violation where the lawyer uses a fake profile to send the friend request (coincidentally this would violate most terms of use agreements with social network providers).

The Ethical Risks of Using “Friend-ing” to Obtain Personal Information

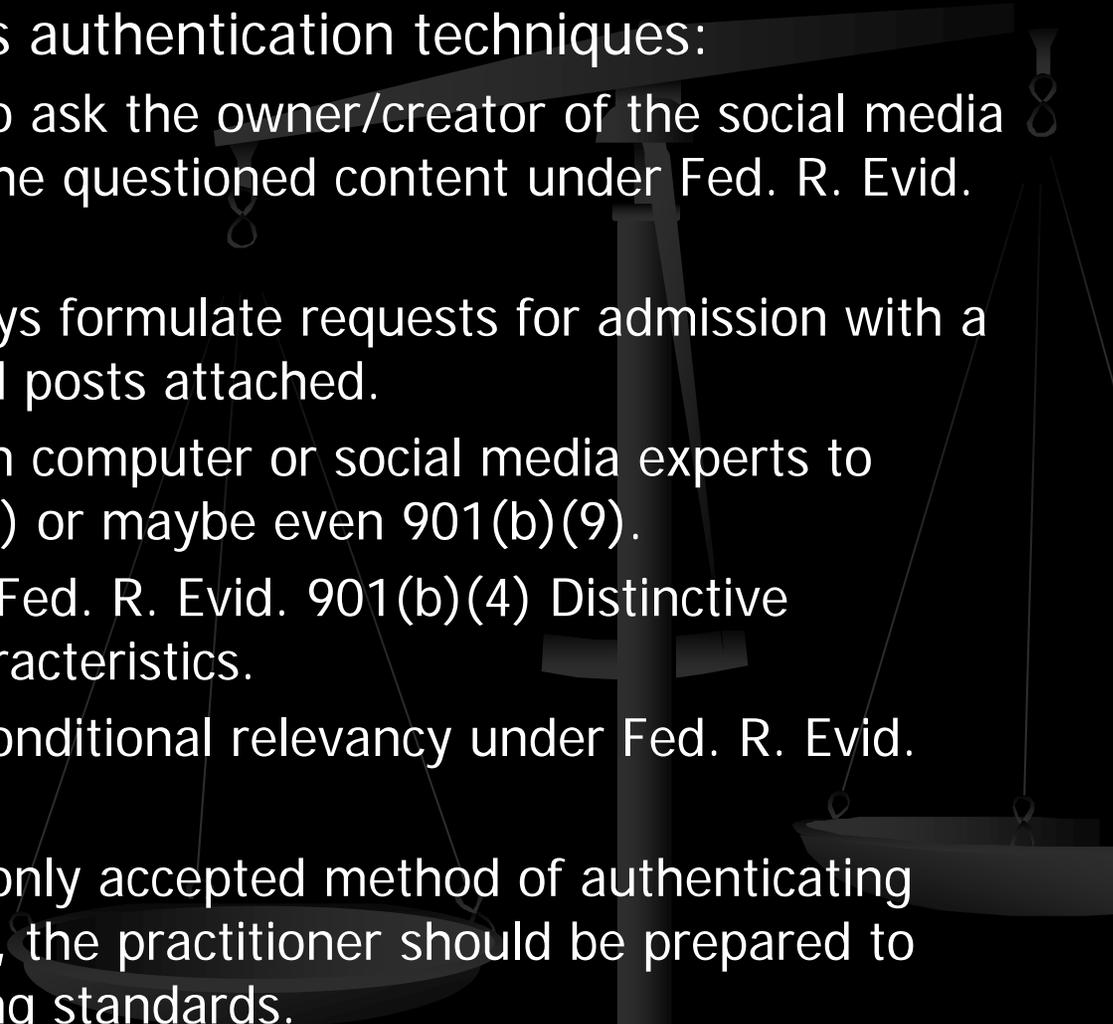
- San Diego Bar Ass’n on Legal Ethics, Op. 2011-2 (2011).
 - Somewhat similar to the Philadelphia and New York opinions, San Diego dealt with a related issue.
 - There the lawyer sought to friend two employees of the defendant’s company in hopes that they would let their guard down over social media.
 - The committee rejected both arguments put forward.
 - It determined that “friend-ing” a represented party is different than accessing an opposing party’s public website.
 - It also found that “friend-ing” is within “the subject of representation.”



Lessons Learned Thus Far

- “Friend-ing” lies on the fringe of many rules
 - Generally, the account from which the request is sent must be valid and truthful.
 - The greater the public access to the profile on which the information is contained, the greater chances that the behavior will be deemed ethical.
 - Greater public access makes the behavior of “friend-ing” more like observing someone in their ordinary course of business. For instance, Facebook may be joined by any member of the public and is thus more likely acceptable.
 - If the networking website is typically reserved for certain groups, the requesting individual, attorney or agent, had better be properly includable in that group to avoid misrepresentation.
- 

Authenticating the Data

- A common objection to social media evidence is found under Fed. R. Evid. 901 that the material is not authentic.
 - Proceed then to various authentication techniques:
 - The most obvious is to ask the owner/creator of the social media profile if they added the questioned content under Fed. R. Evid. 901(b)(1).
 - Second, you can always formulate requests for admission with a printout of the desired posts attached.
 - Third, you can bring in computer or social media experts to testify under 901(b)(3) or maybe even 901(b)(9).
 - Some have also used Fed. R. Evid. 901(b)(4) Distinctive Circumstances or Characteristics.
 - Finally, you can use conditional relevancy under Fed. R. Evid. 104(a) and (b).
 - Until there is a commonly accepted method of authenticating social media evidence, the practitioner should be prepared to meet the most exacting standards.
- 

Cases Dealing With Authentication

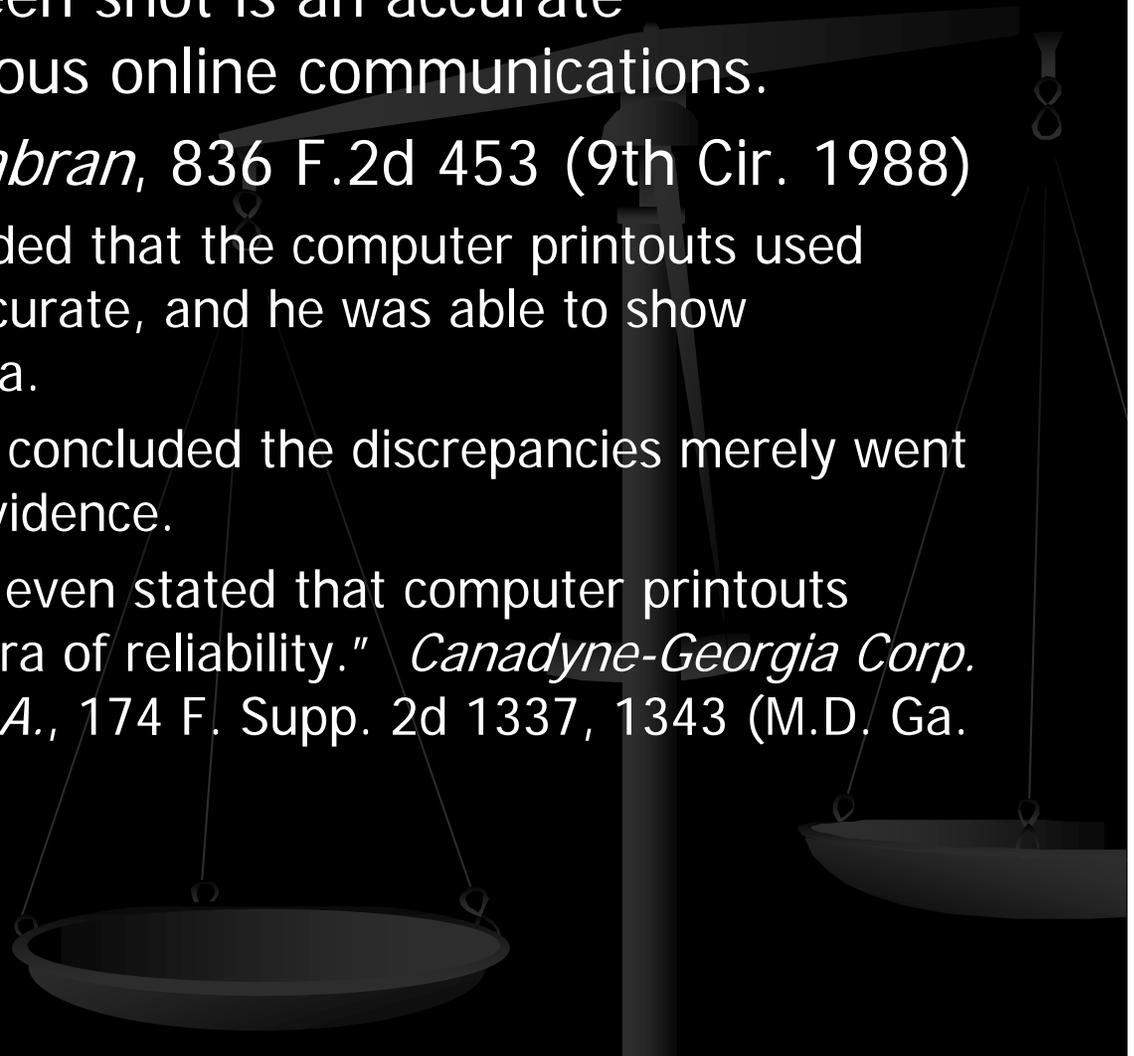
- *United States v. Lanzon*, 639 F.3d 1293 (11th Cir. 2011):
 - The court upheld the admission of transcripts of an instant messaging conversation with an undercover agent.
 - The defendant argued that copying the instant messaging conversations into a word document altered the conversation such that they could not be authenticated.
 - The court rejected this under Fed. R. Evid. 901(b)(1) stating the “proponent need only present enough evidence ‘to make out a prima facie case that the proffered evidence is what it purports to be.’”
- *Griffin v. Maryland*, 419 Md. 343 (Md. Ct. App. 2011):
 - MySpace printout was admitted into evidence as it contained the birth date, photo, number of children, and nickname of the defendant.
 - The trial court stated allowed for authenticating an exhibit by showing that it came from a particular person by virtue of its disclosing knowledge of facts known peculiarly to him.
 - The Maryland Court of Appeals would eventually reverse the decision of the trial court because the “facts known peculiarly to him” could have easily been duplicated by another user in this instance.

Cases Dealing With Authentication

- *People v. Lenihan*, 911 N.Y.S.2d 588 (N.Y. Sup. Ct. 2010).
 - The mother of the defendant in a murder case downloaded photos from the government witness' MySpace page four days after the shooting.
 - The court found the defendant's foundation improper in light of the ability to photo shop, edit photographs, and the fact that the defendant did not know who took the photographs or who uploaded them.
- *People v. Clevestine*, 68 A.D.3d 1448 (N.Y. App. Div. 2009).
 - In another internet sexual assault case, the state presented testimony from a computer forensic analyst and a legal compliance officer from MySpace.
 - The legal compliance officer was able to provide testimony that satisfied the *Griffin* court's concern that the messages originated from the MySpace account, and he satisfied the *Williams* court's concern about access and use of the profile.
 - The court stated that under Fed. R. Evid. 104(b) the "trier of fact could weigh the reliability of the MySpace evidence against the possibility that an imposter generated the material in question."

In What Form To Submit The Data

- Lately, courts have not had great difficulty in accepting that a printout or screen shot is an accurate representation of various online communications.
- *United States v. Catraban*, 836 F.2d 453 (9th Cir. 1988)
 - The defendant contended that the computer printouts used against him were inaccurate, and he was able to show inaccuracies in the data.
 - Despite this, the court concluded the discrepancies merely went to the weight of the evidence.
 - Indeed, one court has even stated that computer printouts "have a prima facie aura of reliability." *Canadyne-Georgia Corp. v. Bank of America, N.A.*, 174 F. Supp. 2d 1337, 1343 (M.D. Ga. 2001).



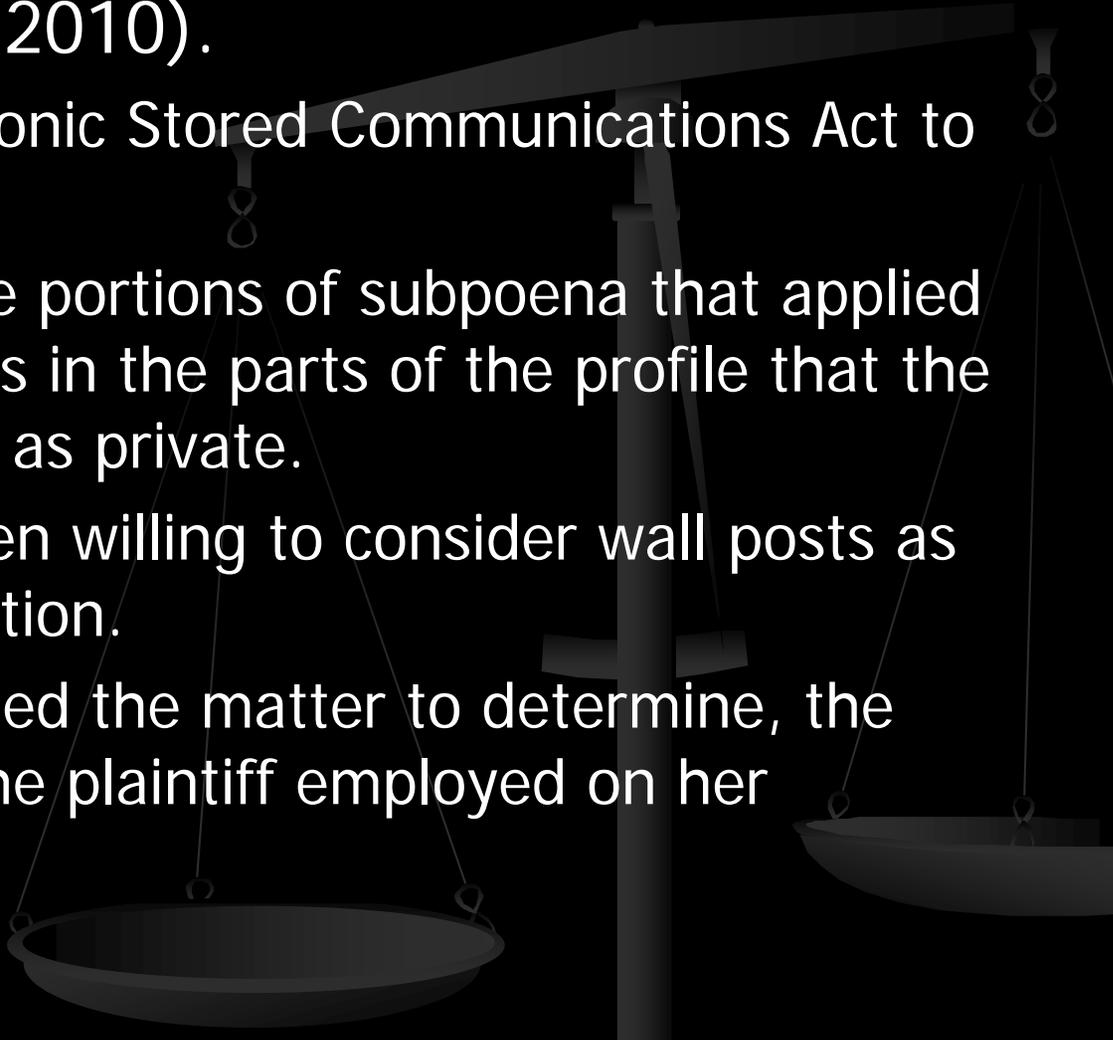
In What Form To Submit The Data

- *Firehouse Restaurant Group, Inc. v. Scurmont LLC, C/A* No. 4:09-cv-00618-RBH, 2011 WL 3555704 (D. S.C. Aug. 11, 2011).
 - The plaintiff asserted that the printouts from various websites could not be properly authenticated.
 - The defendant argued that most of the printouts contained dates and web addresses on them and “courts may consider ‘circumstantial indicia of authenticity’ such as the presence of the date and identifying web address for purposes of authentication.”
 - The court concluded that these distinctive characteristics were sufficient to make a prima facie showing of authenticity.
- Similarly, in *United States v. Tank*, 200 F.3d 627, 630–31 (9th Cir. 2000), it was held that chat room transcripts and printouts, much like emails, could be authenticated by the testimony of one of the participants in the online chat.

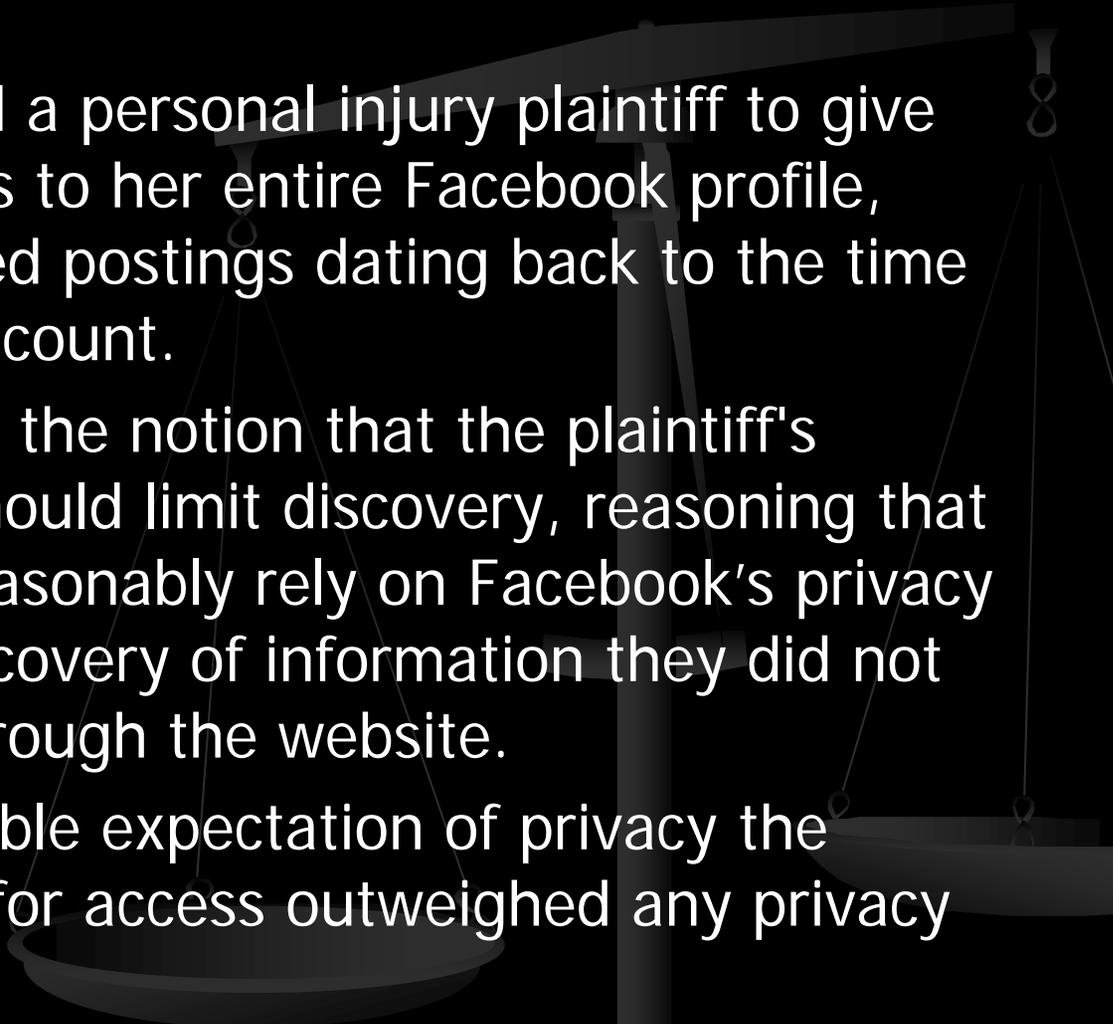
In What Form To Submit the Data

- Social Media has proved a little tougher for courts due to the ability to create a screen name.
- *LaLonde v. LaLonde*, No. 2009-CA-002279-MR, 2011 WL 832465 (Ky. Ct. App. Feb. 25, 2011).
 - Wife argued in custody case that the photographs could not be authenticated “because Facebook allows anyone to post pictures and then ‘tag’ or identify the people in the pictures.”
 - However, the court reasoned that “[t]here is nothing within the law that requires her permission when someone takes a picture and posts it on a Facebook page.” Also, no permission required to be “tagged” in a photo.
 - Wife's testimony that she was the person in the photographs and that the photographs accurately reflected her drinking alcohol was sufficient to meet the standard of authentication.
- All forms of evidence are subject to a possibility of alteration.

Three Commonly Cited Opinions

- *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010).
 - Applied the Electronic Stored Communications Act to Facebook.
 - Court quashed the portions of subpoena that applied to communications in the parts of the profile that the user had selected as private.
 - The court was even willing to consider wall posts as protected information.
 - The court remanded the matter to determine, the privacy settings the plaintiff employed on her Facebook page.
- 

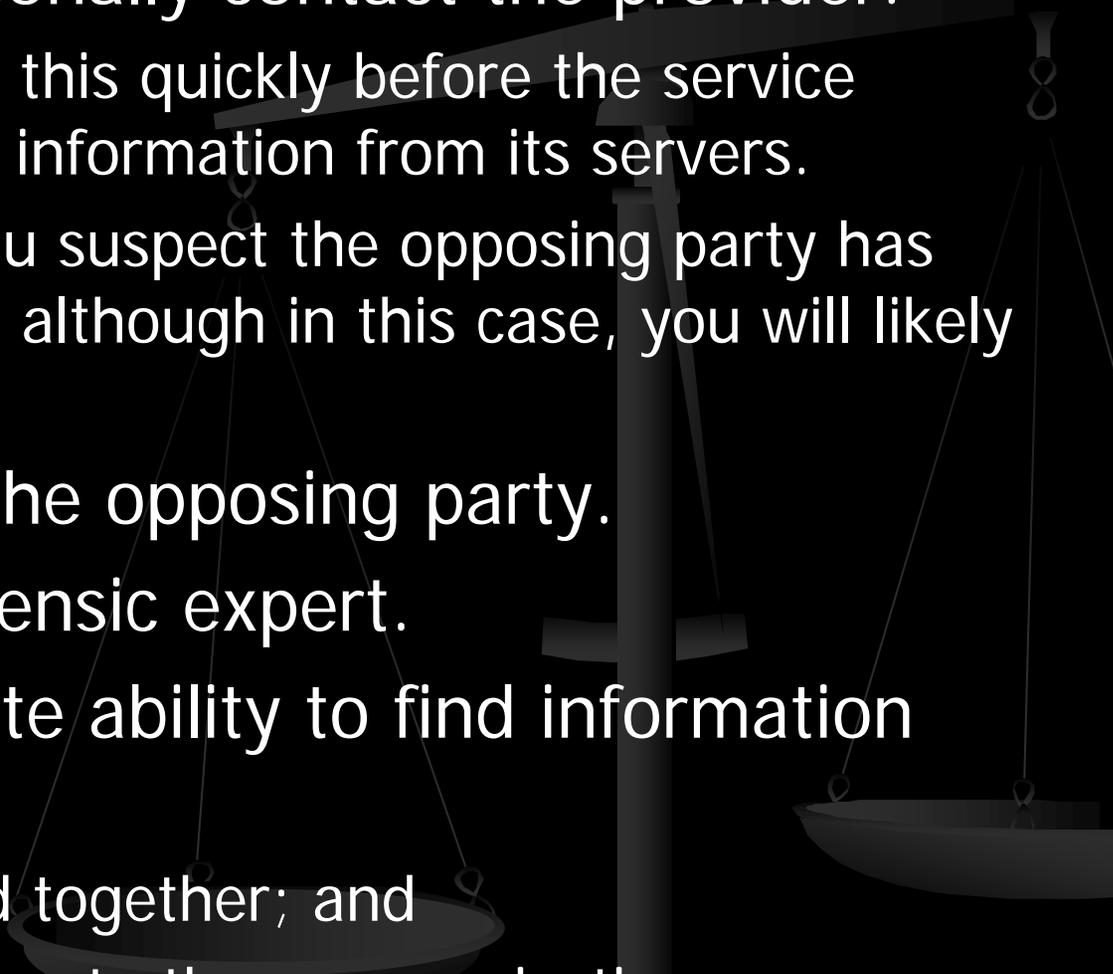
Three Commonly Cited Opinions

- *Romano v. Steelcase*, 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010).
 - Trial court ordered a personal injury plaintiff to give the defense access to her entire Facebook profile, including all deleted postings dating back to the time she opened her account.
 - The court rejected the notion that the plaintiff's privacy settings should limit discovery, reasoning that litigants cannot reasonably rely on Facebook's privacy settings to bar discovery of information they did not intend to share through the website.
 - Without a reasonable expectation of privacy the defendant's need for access outweighed any privacy objections.
- 

Three Commonly Cited Opinions

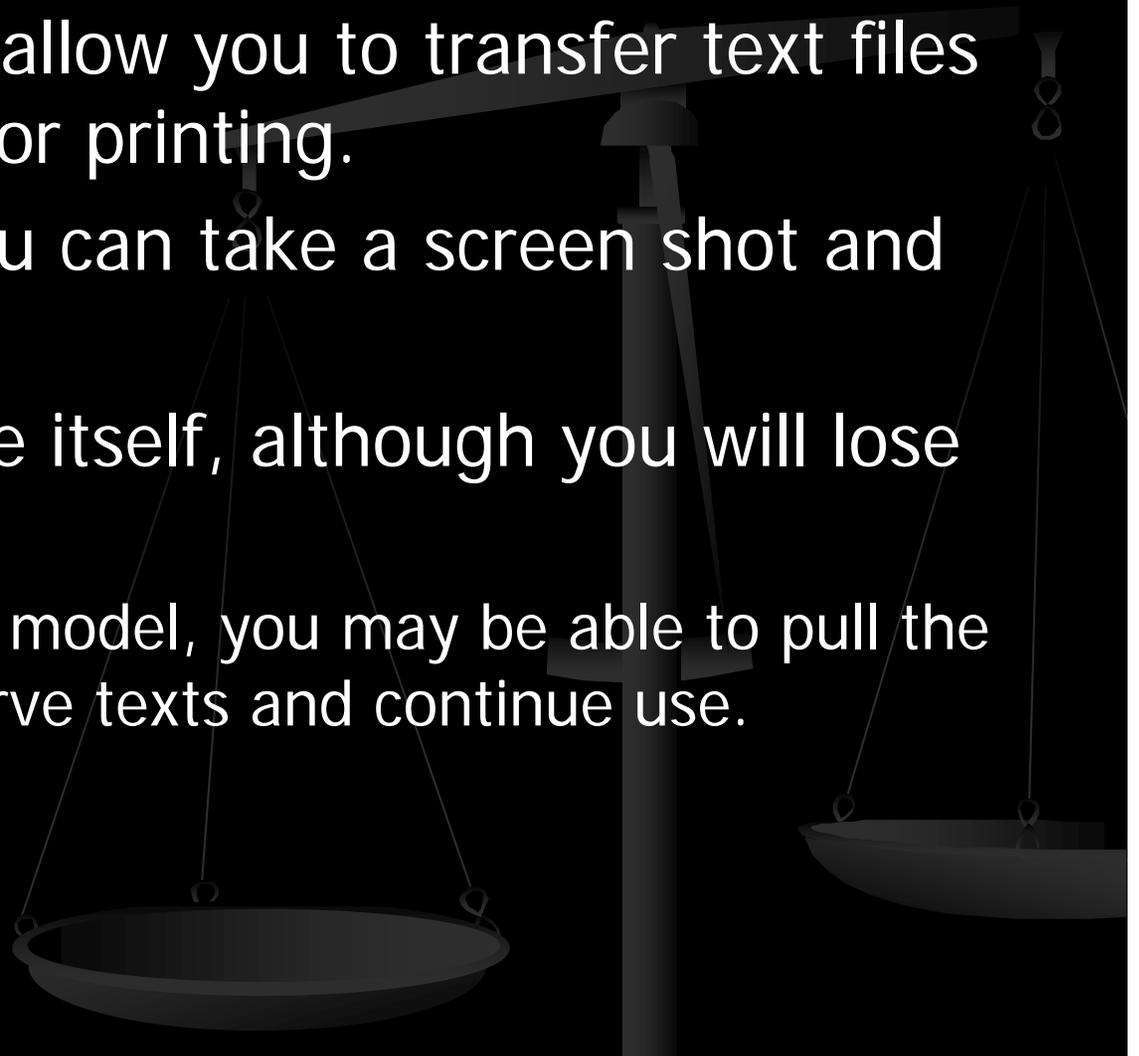
- *Ledbetter v. Wal-Mart Stores, Inc.*, No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *1 (D. Colo. Apr. 21, 2009).
 - Court refused to quash Wal-Mart's subpoenas in personal injury suit aimed at the plaintiff's social media profiles.
 - The subpoenas sought all communications, including private blog entries.
 - Court concluded the subpoenas were "reasonably calculated to lead to the discovery of admissible evidence as is relevant to the issues in this case."
- Most courts, thus far, seem to settle the issue of discoverability on relevance, although after *Crispin* the courts may consider protection under the SCA.

Retrieval Options For Deleted Data

- If you own the device or account in question, you may be able to personally contact the provider.
 - It is important to do this quickly before the service provider deletes the information from its servers.
 - The same goes if you suspect the opposing party has deleted information, although in this case, you will likely need a subpoena.
 - Gain consent from the opposing party.
 - Hire a computer forensic expert.
 - Do not underestimate ability to find information elsewhere.
 - Other Devices linked together; and
 - Other potential parties to the communication.
- 

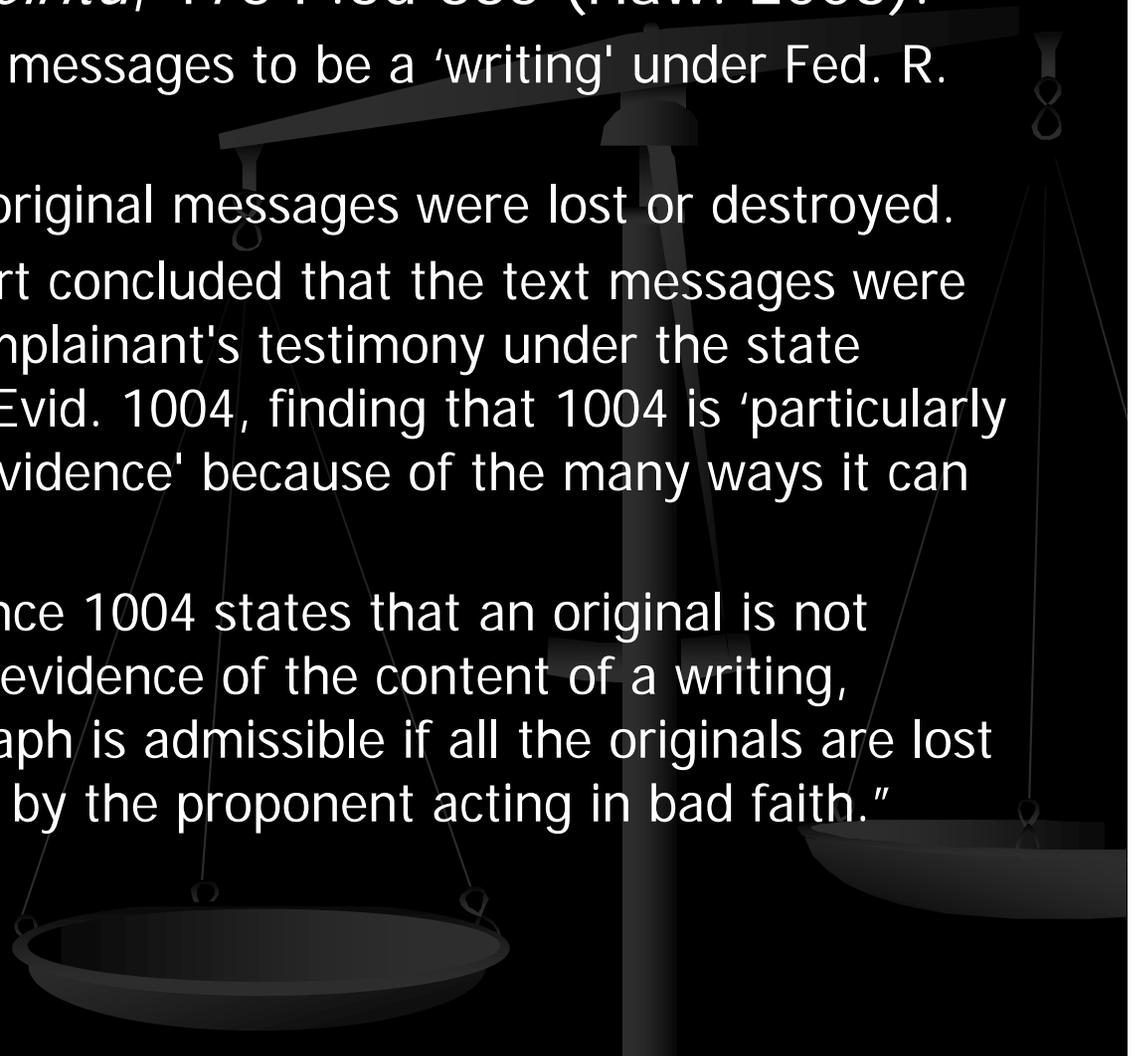
In What Form to Admit Texts

- Printouts of text will typically be sufficient.
- Some phones will allow you to transfer text files onto a computer for printing.
- In other cases, you can take a screen shot and print the photo.
- Can use the device itself, although you will lose use of the device.
 - Depending on the model, you may be able to pull the SIM card to preserve texts and continue use.

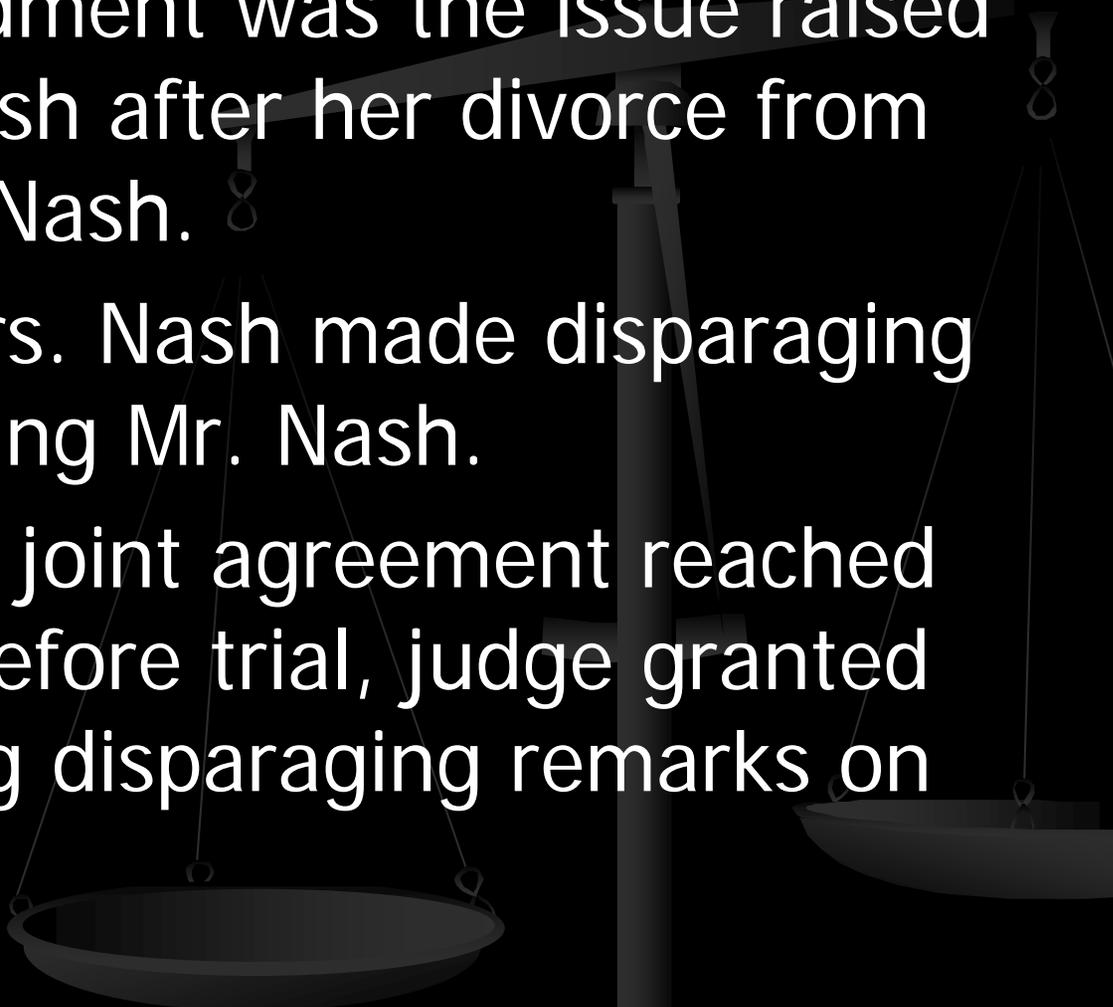


Lessons From Recent Court Rulings

- *State of Hawaii v. Espiritu*, 176 P.3d 885 (Haw. 2008).
 - Court considered text messages to be a 'writing' under Fed. R. Evid. 1002.
 - Court found that the original messages were lost or destroyed.
 - Nevertheless, the court concluded that the text messages were admissible via the complainant's testimony under the state equivalent of Fed. R. Evid. 1004, finding that 1004 is 'particularly suited for electronic evidence' because of the many ways it can be deleted or lost.
 - Federal Rule of Evidence 1004 states that an original is not necessary and "other evidence of the content of a writing, recording, or photograph is admissible if all the originals are lost or destroyed, and not by the proponent acting in bad faith."

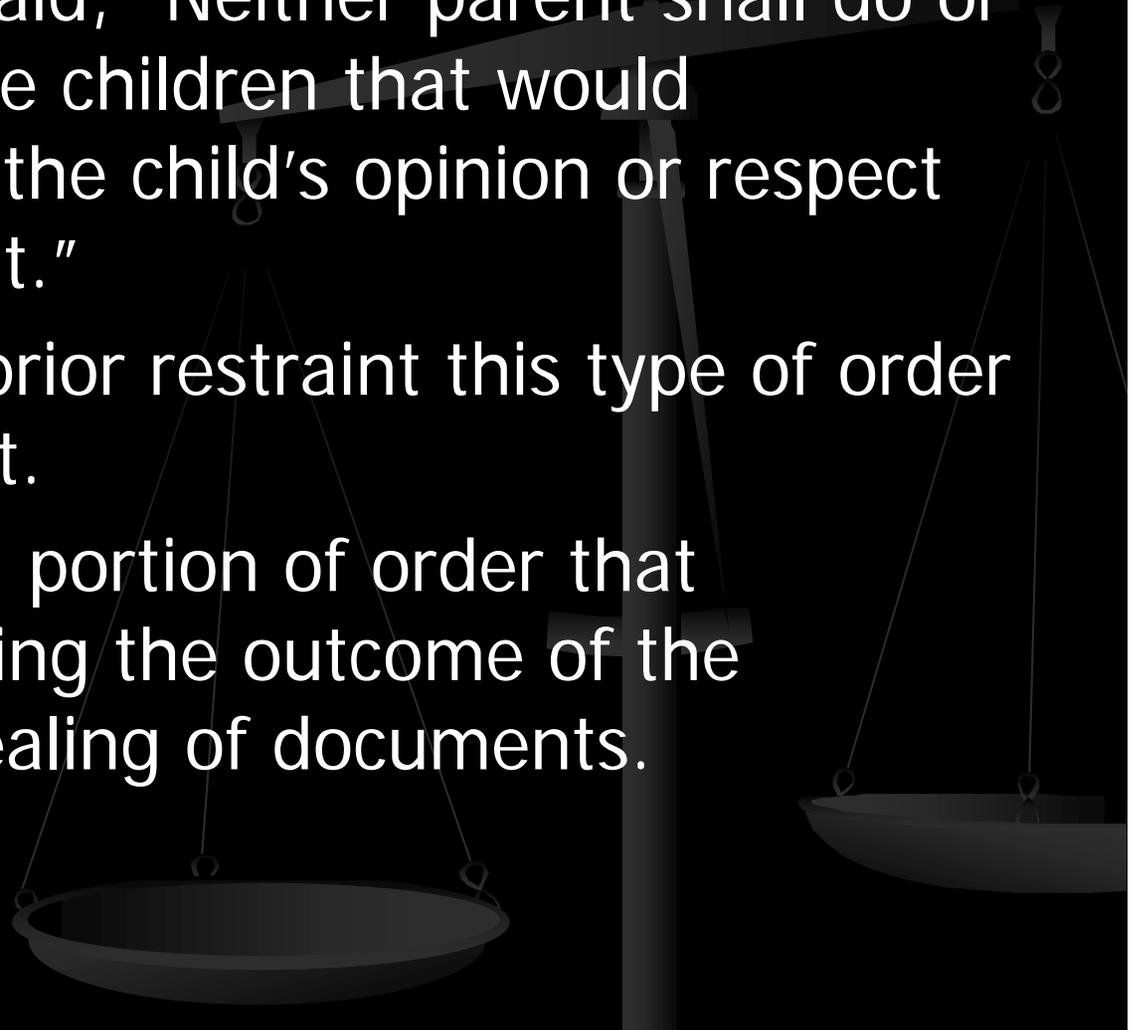


Ex's Disparaging Remarks On Social Media Protected?

- The First Amendment was the issue raised by Alejandra Nash after her divorce from NBA star Steve Nash.
 - After decree, Mrs. Nash made disparaging "tweets" regarding Mr. Nash.
 - After examining joint agreement reached by the parties before trial, judge granted order prohibiting disparaging remarks on social media.
- 

Ex's Disparaging Remarks On Social Media Protected?

- Joint agreement said, "Neither parent shall do or say anything to the children that would negatively impact the child's opinion or respect of the other parent."
- Court noted as a prior restraint this type of order was highly suspect.
- Court struck down portion of order that prohibited discussing the outcome of the proceeding and sealing of documents.



Ex's Disparaging Remarks On Social Media Protected?

- Ultimately, was an exceptional case.
 - Factors for upholding ban on disparaging social media comments were:
 - Content of Joint Agreement;
 - High profile parties;
 - Young children; and
 - Perhaps content of the "tweets" themselves.
 - Moving forward, courts will continue to grant orders prohibiting disparaging comments between the parties, but bans as to social media and 3rd parties will continue to be rare.