

**SMART PHONE & SOCIAL MEDIA EVIDENCE FOR LAWYERS
AND JUDGES**

KIRK C. STANGE, ESQ. *

* Special thanks to Jeffrey Klaus for helping prepare these materials.

I. WHAT TO LOOK FOR AND WHERE TO FIND IT

a. SOURCES OF DATA

The conventional ways to obtain information in divorce proceedings are well known: (1) Interrogatories; (2) Requests for Production; and (3) Depositions. Typically, interrogatories are aimed at gathering initial information and facts of the case that the opposing party could not recall without reference to particular documents.

Interrogatories in conjunction with requests for production, then serve to produce the traditional sources of information for a divorce attorney. Staples include:

- (1) Bank Statements;
- (2) Individual Tax Returns;
- (3) Corporate or Partnership Tax Returns;
- (4) Mortgage Statements;
- (5) Rental or Lease Agreements; and
- (6) Telephone Records.

These documents can then be used in conjunction with depositions to “pin” down the testimony of the opposing party for potential impeachment at trial, or simply to see how the opposing party will respond under oath to particular questions.

Now, however, we have a broader array of materials with which we can target these traditional discovery tools. These new materials can be used for the same purposes, but they often pose new challenges. They include, but are not limited to:

- (1) Home and Work Computers;
- (2) Cell Phones and Tablets;
- (3) Flash Drives and External Hard Drives; and
- (4) Cloud Storage/Vendor’s Servers.

Many Computer and E-discovery issues are covered by federal statutes and the Federal Rules of Civil Procedure. However, it is also vital to check local rules of civil procedure in your jurisdiction. Below are various applicable Federal Rules of Civil Procedure that sometimes mirror state rules:

Fed. R. Civ. P. 1001(1) - Writings and recordings includes computers and photographic systems.

Fed. R. Civ. P. 26(a)(1)(C) - Obligates parties to provide opponents with copies of or descriptions of documents, data compilations, and tangible things in a party's possession, custody, or control.

Fed. R. Civ. P. 34 - Permits a party to serve on another party a request to produce **data compilations** (subpoena). This can include word processing files, spreadsheet files, investment data or databases, calendars, browser histories, contact lists, digital photographs, email and social media. These and other miscellaneous information can be found on: hard drives, floppy disks, optical disks, flash drives, network storage, remote storage, cell and smart phones and virtually any electronic source.

Note: Often these may be the only place where evidence exists on a particular issue.

1. Home and Work Computers

The overarching federal statute is 18 U.S.C. § 1030 or the Computer Fraud and Abuse Statute. Section 1030 prohibits (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; (c) intentionally accessing a protected computer without authorization, and as a result of such conduct, causing damage. A protected computer is any computer used in interstate or foreign commerce or communication, which is obviously quite broad, but the key in family law cases is typically "use without authorization." Wiretapping statutes and Electronic Communication Privacy Act also come in to play with email discovery and will be discussed later.

State Courts have been all over the place on the balance between privacy and discoverability. Below are a few examples:

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 took the computer to her lawyer to have its memory copied. The real issue was not who possessed the computer, but who had access to 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 a file cabinet left in the marital residence. Likewise, she should have access to the contents of the computer.

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 notebook as a list of adulterous encounters.

State v. Appleby, 2002 WL 1613716 (Del. Super. Ct. July 18, 2002): Here, husband and wife routinely commingled computer hardware. Despite wife having possession at time of trial, it was "theirs" in every sense.

The balance then between privacy and discovery appear to revolve around, first, whether it was marital property or was used by others in the home. The proponent is likely to encounter greater resistance if the information was password protected. Second, if it was not marital or readily used by others in the home, is there some credible reason to suspect relevant evidence will be discovered? Case law seems to indicate that you must have more than a mere suspicion, but it cannot hurt to try because on appeal it is often all about the standard of review. Frequently, an appellate court will be resistant to state that the trial court abused its discretion.

2. Cell 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).

The most common application for cell phones in a divorce matter is to subpoena the carrier for itemized billing. This is 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 akin to a computer.

3. 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. An external hard drive may be set up to automatically back up any files saved on the main computer and may be worth looking at if you suspect something is missing from the main drive. An external hard drive may be composed of one of many types of memory, but typically are a hard disk drive like those found in a traditional computer. External hard drives with the capacities of up to a massive 8TB of storage (1TB equaling approximately 140 million pages of text) can now be purchased readily by consumers.

A hard disk drive records data by magnetizing a thin magnetic material on a spinning disk. It may be important to know what type of drive is used in a computer or

externally because when you delete a file in windows it does not remove the magnetic coding from the disk. Deleting merely removes the location of that file from the directory with which an application would access it. The file itself may remain there undisturbed until a later application saves something over it.

The flash drive is probably the biggest competitor of traditional hard disk drives. Originally invented in 1980, they have rapidly gained in popularity for their portability and durability. Flash drives unlike their hard drive counter parts, do not have any moving parts and can retain data without a power source. They typically connect to a computer through a USB port and boast an impressive capacity of up to 2TB in 2013. Flash drives, like a hard drive are often re-writable, and memory deletion typically operates in a fashion similar to hard disk drives.

Similar to a computer, a spouse may have a right access to an external hard drive or flash drive used in the home, but 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.

4. Cloud Storage

While over the past decade courts have to some extent learned to cope with electronic discovery from computers, cell phones, and extra storage drives, cloud services present a few new challenges. The National Institute of Science and Technology defines Cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” 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 has its advantages for users, and disadvantages for litigants. Cloud computing is growing rapidly for good reason. It 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. It is the limitless capacity and lack of self management that poses the challenges for litigants. While computer hard drives now contain vastly more data than ever before, creating even more items of evidence to sort through, cloud storage only exacerbates that difficulty. The particularly interesting aspect is the lack of direct control the cloud user typically has over his or her stored data.

Traditionally, companies stored and owned their own data located at specifically constructed data centers. Even if the company or individual leased the space, they at least owned the hardware and data itself. Cloud services change this to where the user no longer owns the hardware they operate. Cloud services follow three basic service models. The most general model is the Software as a Service (SaaS) model where an individual pays only for existing applications in the cloud. The user has no control over how data is stored or altered within the system. For lawyers, a familiar example of this is Westlaw or LexisNexis. The second model is the Platform as a Service (PaaS) model, which gives the user the ability to install and tailor their own software applications in the cloud. The user still, though, has no control over the servers or storage provided. Finally, the Infrastructure as a Service (IaaS) model offers clients the most control. There the user rents access to the cloud's servers and hardware, but may use its own operating system and software that enables the cloud to work for the user. Importantly, the service provider may still re-locate data from one physical location to another.

The ability of the cloud provider to re-locate data becomes important in looking at 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). The problem

that generally arises though is locating and preserving the data for pending litigation. Third party control, through a cloud, may leave the user subject to sanctions when the data has been moved, altered, or is otherwise inaccessible.

In discovery, the responding party has the burden to preserve, identify, and collect ESI stored in the cloud. While the comments to Fed. R. Civ. P. 37(e) states “A preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case,” and it also states that the duty to preserve evidence attaches when the party reasonably anticipates litigation. For those operating under any cloud model but the IaaS model, a responding litigant will not be able to prevent any auto-delete functions associated with the cloud. Important data may also be lost if the service provider chooses to terminate cloud services provided to the user. For instance, Amazon’s 2012 service agreement provided that termination of the agreement terminated all rights to any of the data stored in the cloud.

This inability to retrieve ESI from the cloud may trigger sanctions for the responding party. Court may impose sanctions for spoliation under Rule 37 when they deem it just. The standard seems to vary by circuit, as some will grant a sanction if the responding party is culpable in any way, which is if they have any responsibility or control. Other courts require a showing of bad faith.

Under either standard, it is important that you know the cloud structure and operating methods that your client employs. Having a basic knowledge of your provider will help you negotiate the service agreement to begin with, locate data when the time arises, and ensure that the data is unaltered when it comes time to produce. Moreover, it will enable you to create a prospective litigation plan that may save you time and money in the future.

If you are the party requesting data from the cloud, a basic idea of how the cloud operates will also be useful. It may inform you that the targeted party does have significant control over their data as they are employing an IaaS cloud model or that the documents or the meta-data contained in the documents you have received may have been altered in the cloud. It may even tip you off that other documents may have been

deleted, perhaps innocently, while contained in the cloud. Either way, a rudimentary knowledge of the opposition's system will only help your discovery efforts.

b. TYPES OF DATA

These new sources can be used to target pieces of information beyond those found in the traditional sources of information. The amount of electronically stored information today is staggering compared to say just twenty years ago. This is because, in 1990, the cost of storing a gigabyte of data was approximately \$20,000 while today that cost is under \$1. This wealth of information is becoming increasingly available for attorneys in dissolution proceedings. Today, in divorce litigation, the primary costs come from reviewing all of the data out there and that counsels a thoughtful approach. Securing access to these sources of data may lead to the discovery of:

- (1) Emails;
- (2) Cell phones and Text messages;
- (3) Social Media Use;
- (4) Browser History; and
- (5) Geolocation Data.

It is then important to determine which of these may provide your client with the most pertinent information.

1. E-Mail

The use of email by opposing spouses falls within the interplay of wiretapping and electronic stored communications laws, and consequently, courts have had some difficulty in determining which, if any, apply. The predominant approach seems to be that emails prior to being sent or once received do not fall within wiretapping statute. Take for example *Evans v. Evans*, 610 S.E.2d 264 (N.C. Ct. App. 2005). There, 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. (citing *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2003).

However, one Florida Court has concluded that spyware capturing emails in a family law case did violate ECPA and admission of these emails was within the discretion of trial court. *See, O'Brien v. O'Brien*, 899 So.2d 1133, 1138 (Fla. Dist. Ct. App. 2005). In this case, the court granted an injunction against using or disclosing the information gained.

Most spyware/keystroke capture programs remain legal, as long as they are not capturing contemporaneous transmission of communication (outside of Florida). It is not, however, wise to advise a client to use these because the law on the topic is vague. You can counsel your client to search for spyware planted by the opposing party, but often such programs are not really there.

With further regard to the discovery of emails, subpoenaing internet service providers will typically only generate the sender and recipient of a message. ISP's, like cell phone providers, often delete this information quickly. However, certain service providers do retain the data so it may be worth the attempt.

2. Cell Phones and Text Messages

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).

The most common application for cell phones in a divorce matter 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. As many people now communicate far more frequently through text

message than phone call, these may provide an excellent source of information when it comes to proving the behavior of the opposing party.

Outside of intercepting telephone conversations or voicemails, smart phone data and tablets are akin to a computer.

3. 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. People often use these websites daily, which contain a treasure trove of information. As proof of this, eighty-one percent of American Academy of Matrimonial Lawyers (1600 surveyed) recently reported increased use of social media evidence. The reason for this is that discovery utilizing these websites may reveal: postings that display a time line of actions; 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/or extreme ideologies or beliefs.

4. Browser History

There are numerous software applications out there, commonly referred to as web browsers, which are used to navigate the internet. Browsers interpret the URI or URL and allow you to access the content on a webpage. Browsers can also be used to navigate web servers in private networks or files in file systems. Common examples include: Microsoft's Internet Explorer; Google Chrome; and Mozilla's Firefox. If the client has a right of access to the computer, it can certainly be worth investigating the browser history, or if not, it may be an excellent choice for a targeted subpoena.

Most of us are familiar with the idea that our web browsers track a history of the websites we visit. This is often a matter of convenience, so that we do not have to continue to remember unwieldy URL's. Web browsers typically delete the history of web pages visited after a given period of time and manually removing the history is also easily accomplished.

What is to some extent lesser known, is that when your web browser accesses a file on the internet it “caches” it, or stores it. The browser does this so that when you click on the back or forward tabs, the software application does not have to re-retrieve the data. This cached file is essentially a snapshot of the web page and may include text and any images on the webpage. Here, too, cached files can be manually deleted, but this is less likely for the computer novice.

Along with cached files, your web browser will create cookies at the request of the website. Cookies are stored on your computer and contain user specific information so that the website can re-access that information when the user re-visits the site. These files allow the website to personalize the user’s visit or speed up the user’s authentication by remembering passwords. Cookies can even contain the web address the user visited before entering its website. In some operating systems, a cookie will also reveal the user who was logged in when the website was accessed. Also, clicking on the file’s properties will reveal the date the cookie was created and the date the site was last visited.

Many browsers will automatically clear cookies after they have reached a certain age, but to a computer forensic, cookies may provide insight into the user’s online behavior. The ability of the cookie to speed up authentication can allow one to copy it and enter a website as if you were the originating user. While this may be problematic as an offensive strategy, it may prove a useful defense when claiming your client was not the individual accessing the website. Also, a file called INDEX.DAT provides a subdirectory of cookies which lists at least a partially plain text listing of every website that dropped a cookie on the system.

5. Geolocation Data

In the last quarter of 2010, for the first time, mobile phones outsold personal computers. This is important because by the end of 2005 cell phone providers were tasked with making calls “location capable” for 911 services. This meant that cell phone usage needed to be traceable to within 300 meters. While in prior years, location data was pulled from cell phone towers, today nearly every phone is equipped with a GPS

device accurate within a few meters. Also, today's phones are WiFi capable, which means they also store data about the networks they are using.

All of these: cell tower data, GPS, and WiFi serve to create geolocation data. They create a record of where you were and when. The previously discussed sources of information: emails, text messages, and social media, all provided subjective information about your location (i.e. Tom said he was at the cafeteria late last night). The data provided by cell phones and GPS enabled apps provides objective evidence that Tom was not at the cafeteria late last night. Moreover, most GPS enabled camera phones also embed the longitude and latitude data of photos when they were taken (many apps exist for converting latitude and longitude into a street address). This data known as Exchangeable Image File Format (Exif) metadata 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.

This also means that even a stationary computer can be important in terms of geolocation data. The computer itself reveals its location and the user's during use, but also it contains a litany of files that may contain geolocation data. Moreover, many tablets or smart phones can be synced with the computer as a sort of back up drive. This means that all of the geolocation data stored on the phone or tablet, may also be found on the home computer. This can be particularly important if the spouse has a right of access to one device, but not another.

c. WHAT TYPE OF INFORMATION TO LOOK FOR

Simply put, what to look for depends on what type of case you have and what types of allegations you are seeking to prove or disprove. Knowledge of what you need to prove your point is crucial because of the volumes of potential ESI out there. Not only will a broad meandering search waste a lot of your client's money, but also such attempts are likely to be characterized as an impermissible fishing expedition by the court.

Let traditional sources inform your use of new electronic sources. If you would typically subpoena bank records and credit card statements you might consider examining a computer's spreadsheets for financial information. Or, perhaps you would

consider looking for emails to or from known business associates. If you are looking to prove some sort of conduct between the parties, you might start with emails and text messages. Communications might provide for abundant examples of verbal abuse or promises broken. If allegations of substance abuse or adultery have been leveled, you might consider mining for geolocation data that can show husband or wife was at the bar instead of the soccer game. Finally, consider often overlooked aspects of social media, like status updates and friends lists. The uses for ESI are as broad, if not broader, than the traditional sources of information.

This means you even need to be efficient once you locate your ESI source. Careful selection of keyword searches can be crucial to obtaining information relevant to your case. Through the various social networking web pages valuable information can be obtained regarding adverse parties, key players in your case, and expert and non-expert witnesses. Keyword searches can be performed in various search engines, including Google, Yahoo or Bing. Research can also be performed on Westlaw. Through these vehicles, you can often find invaluable information including contact information, employment information, social information, and habits of various parties in your case.

There are some important basics to know about key word searching. For instance, it can sometimes be wise to focus on items most likely to be discarded or overwritten first, like emails and instant messages. When doing so, and in searching in general, consider the Who, What, When, Where, Why, and How of your case. Be sure to remember assistants or those who may handle your target's files or emails. Additionally, if at all possible, remember to discuss with the custodian of the system possible abbreviations used by the party in question. Try to focus on important dates which might help sift through potentially voluminous amounts of information. Finally, do not be over confident in your search abilities based on Google, Yahoo, Bing or even Westlaw experience. Sifting through data on a computer can be an entirely different animal, so here are a few additional suggestions to fashion queries:

- (1) Start with pleadings, interrogatories, and requests for production to see what information you already have;

- (2) Seek Input from key parties and witnesses;
- (3) Examine what you've got and the tools you will use;
- (4) Communicate and collaborate;
- (5) Incorporate likely misspellings, abbreviations and synonyms;
- (6) Filter and duplicate first;
- (7) Tweak the queries and retest; and
- (8) Check the discards.

If the opposing party is somewhat cunning or deceptive, you might need to partake in a somewhat more detailed examination.

d. PROS AND CONS OF USING OUTSIDE INVESTIGATORS

The Pros: The advantages of hiring an outside investigator can be numerous. To begin, if well selected the individual will be a professional at their trade. In terms of e-discovery, this means that the expert may be able to find all sorts of deleted data from financial records to stored emails. Sometimes this information has not even been deleted, it merely requires someone with the right know how to uncover it. Also, there are instances in which hiring a professional forensic computer analyst to examine a computer or hard drive is the only way important evidence can be found. Useful information may come from unexpected sources as even “meta data,” which is really data about data, can provide the “smoking gun.”

Other advantages are that professionals can access and often mirror a computer or device without damaging any of the files or hardware. This is something even an experienced attorney cannot always be certain of. Also, the process is usually pretty quick. A forensic image of a hard drive often only takes four to six hours and a comprehensive report from a forensic examiner usually takes between two to four weeks. Finally, a forensic report can be a very useful way to prove spoliation of evidence.

The Cons: As with anything, hiring an outside investigator has its disadvantages as well. First and most obvious is that the process can be expensive. Often there are charges for the duplication of any device or hard drive, additional charges for any forensic report produced, and yet more fees for the expert to provide testimony at trial.

Moreover, there is no guarantee that the expert will find anything. This may be because the party has used sophisticated programs to wipe out data or obscure data such that even an expert cannot identify it. Also, and perhaps commonly, there is the risk that there is simply no incriminating evidence to be found on the device.

Further, it is a good idea to make certain that the individual you are hiring really is an expert. You do not want to damage potentially valuable evidence merely because you hired the first person you found who claimed to be knowledgeable about computers. It is even better if they have some idea of the law and admissibility standards.

Finally, if using an outside investigator to examine computer hardware, you must maintain the chain of custody. Check your local standards, but typically shipping via Fed-Ex with a tracking number will suffice.

e. CASE LAW UPDATE

Quite often, social media evidence and electronic evidence in general is the icing on the cake in divorce litigation. For instance, in *In re Marriage of Bates*, 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.” 817 N.W.2d 32 (Iowa Ct. App. 2012). 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. At trial, the wife claimed the emails were influenced by her medications and stress; and on appeal, the court rejected her subsequent assertions that the emails had been altered.

Highlighting the ever changing view of courts on social media evidence *Romano v. Steelcase*, which allowed the discovery of an entire Facebook profile, was recently disagreed with by the Federal Eastern District of New York in *Giacchetto v. Patchogue-Medford Union Free School District*. 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010); No. CV11-6323(ADS)(AKT), 2013 WL 2897054, (E.D. N.Y. May 6, 2013). In *Giacchetto*, the federal judge examining claims both under federal and state law held that only the social

media postings, which referenced events alleged in the teacher's complaint, were relevant and discoverable.

Social media content can be helpful in unexpected ways, like proving the size of a business. In *Safdar v. AFW, Inc.*, the plaintiff filed suit against former employer to recover unpaid overtime wages under the Fair Labor and Standards Act. 279 F.R.D. 426, 430 n. 41 (S.D. Tex. 2012). The cause was submitted on affidavit, and plaintiff used print outs 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.

Additionally, in *Blade v. Harrah's Entertainment, Inc.*, the plaintiff in an age discrimination case was able to use LinkedIn to show that he was indeed an employee of Harrah's. No. 2:08-cv-02798-BBD-cgc, 2010 WL 538746, at *1 (W.D. Tenn. Dec. 17, 2010). His supervisor had testified in court that neither he nor the plaintiff were employees of Harrah's, but after the supervisor's LinkedIn profile listed Harrah's as his employer, the court found the supervisor to lack credibility. At least one court has held that threats posted by a defendant on a social networking website were "sent" to the recipient. *O'Leary v. State*, 109 So.3d 874 (Fla. Dist. Ct. App. 2013).

Social media evidence can also prove to be the tipping point even when alone it is insufficient for the judge to rule in your favor. In a divorce action, wife placed a motion for default on husband's desk in marital home. *Leenhouts v. Leenhouts*, No. M2012-01844-COA-R3-CV, 2013 WL 3968159, at *2-*4 (Tenn. Ct. App. July 31, 2013). Husband, several days later, placed messages on Facebook to the tune of "you thought you had me" followed by several expletives. While the 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.

The Stored Communications Act ("SCA") can also come into play in a variety of electronic discovery settings. An "electronic communication service" ("ECS") is defined

as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” A “remote computing service” (“RCS”) is defined as one that provides “computer storage or processing services by means of an electronic communications system.” ECS providers are prevented from knowingly disclosing the contents of an electronic communication while in electronic storage by that service. A provider of a remote computing service is permitted to release the contents of a communication to the addressee or intended recipient, but cannot disclose electronic communications carried or maintained by that service solely for the purpose of providing storage or computer processing. Several courts have held that data held by an ECS are exempt from the reach of subpoenas in civil actions. *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 611–12 (E.D. Va. 2008).

While not considered in *Romano v. Steelcase*, in *Crispin v. Christian Audigier, Inc.*, the court applied the Electronic Stored Communications Act to Facebook in quashing the portion of subpoena that applied to communications in parts of the profile the user had selected as private. 717 F. Supp. 2d 965 (C.D. Cal. 2010). The court held that general postings viewable to the public on Twitter or Facebook were discoverable, but private messages where the website was acting as an ECS were not.

SCA also complicates the acquisition of location data from an ECS or RCS service provider. A company might be an ECS under the SCA even without providing communication services to the public. *See Devine v. Kapasi*, 729 F. Supp. 2d 1024, 1026-28 (N.D. Ill. 2010). But customers can obtain their own data from an ECS and RCS. Some courts have ordered customers who are civil litigants to request data from ECSs and RCSs that could not be subpoenaed directly by the non-customer or opposing party under the SCA. *See Fhigg v. City of Detroit*, 252 F.R.D. 346, 357–58 (E.D. Mich. 2008).

In *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. Similarly, in another case, the plaintiff’s supervisor

proceeded to read previously read personal, but not deleted emails, on a former employee's blackberry. *Lazette v. Kulmatycki*, No. 3:12CV2416 2013, WL 2455937 (N.D. Ohio June 5, 2013). 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-mail, because it was the server that was the protected storage device, not the smart phone.

In *White v. White*, the wife hired a computer expert to find and copy her husband's e-mails that were stored on the hard drive of the computer in the family home. 781 A.2d 85 (N.J. Super. Ch. 2001). The court held that the wife did not violate the SCA, because it determined the e-mail was not in electronic storage when it was accessed because the computer hard drive was not electronic storage. They also determined that the access was not without authorization.

Perhaps signaling a trend with regard to the admissibility of geolocation data the court in *United States v. Walker*, 771 F. Supp. 2d 803, 810–11 (W.D. Mich. 2011), justified the GPS device attached to the bumper of the defendant's car by saying the attachment was 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.

Bear in mind as well that often it is harder to destroy ESI than it is to assure that it has been retained. For instance, in *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. This also shows that sometimes carriers retain text data.

Confirming that proving spoliation may be difficult, the court in *PTSI Inc., v. Haley*, refused to issue sanctions for spoliation of messages on a phone. 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 not awarding sanctions based on the deletion of emails.

II. FACEBOOK DISCOVERY HOW-TO'S

a. SUBPOENAING FACEBOOK FOR RELEVANT RECORDS

Once you have decided that social media content will be or could be important to your case, you have several initial options. First, you can obtain the consent of the other party to produce the requested data. Second, you can attempt to subpoena the provider. Finally, you can attempt to compel the opposing party to produce the data.

Your best two options are typically to acquire consent or to subpoena the opposing party. If you subpoena the opposing party, you may be forced to explain to the judge why such materials are relevant, and you may have difficulty with access and the formatting of information. Users are only able to provide the information in screenshots and may not even have access to all of their historical data. Even still, user consent or a subpoena to the user may be your best option, because often social media providers are not particularly cooperative, and even if they are helpful, they are still expensive. For example, Facebook, at one time, charged a non-refundable \$500 processing fee in addition to a \$100 notarized declaration of the records authenticity. Additionally, in the case of Facebook, you need either a valid California or federal subpoena.

Even if you are successful in subpoenaing Facebook, you may receive limited information. The company has over 30,000 servers located in several data centers across the United States. 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.” Some speculate that in the wake of *Crispin* and the SCA

that 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." Now, an individual's entire Facebook profile is downloadable by the user, thus mitigating the need to subpoena the provider.

Other social media websites, such as MySpace, pose even greater difficulties as they require additional information, such as user id, password, and birth date. Even once you have gathered such information, you are likely to run into issues with what information contained in the profiles is discoverable.

b. WHAT CAN BE DONE IF THE ACCOUNT'S BEEN CLOSED?

What to do if the account has been closed? Facebook's policy states: "If a user cannot access content because he or she disabled or deleted his or her account, Facebook will, to the extent possible, restore access to allow the user to collect and produce the account's content. Facebook preserves user content only in response to a valid law enforcement request." Facebook's website states that it takes approximately one month for an account to be deleted, but also states that some information may be contained in back-up copies for up to 90 days. Further, even if an account has been deleted, some pieces of information like messages or group postings will remain because they are not stored on your account. If an account has merely been de-activated, as opposed to deleted, Facebook will retain all of the information in the profile indefinitely in case you choose to re-activate. You may be able to distinguish between the two, because if the account is merely de-activated, the user will still appear on others' friends lists.

What this means is that all is not lost when the opposing party responds with "what Facebook account?" If your client can still see the target on their friends list, you know the account is merely deactivated. This means, it could be reactivated and downloaded by the user or that you should expect data, if Facebook were to comply with

your subpoena. Even if the account has been deleted, you know you stand a decent chance of still acquiring some information for a period up to 90 days. Even after 90 days you might be able to acquire data from other users who communicated with your target.

c. THE ETHICAL RISKS OF USING “FRIEND-ING” TO OBTAIN PERSONAL INFORMATION

Many have probably considered “friend-ing” someone to avoid having to seek consent or to avoid the cost of subpoenaing social media outlets and their users. This, however, is a dangerous proposition because the vast majority of states have adopted the Model Rule of Professional Conduct 8.4. Rule 8.4 makes it professional misconduct for any lawyer to engage in dishonesty or misrepresentation. The rule also makes it misconduct for a lawyer to supervise anyone in activity that would be misconduct if partaken by the lawyer. Thus, it would seem that “friend-ing” an opposing witness or even worse an opposing party would likely violate this rule (communicating with the opposing party would also violate Rule 4.2).

Specifically, two bar opinions have addressed this issue. The Philadelphia Bar Professional Guidance 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. Phila. Bar Ass’n Prof’l Guidance Comm., Op. 2009-02 (2009). Contrary to this, the Bar of the City of New York Committee on Professional Ethics 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.” N.Y. City Bar Ass’n Comm. On Prof’l & Judicial Ethics, Formal Op. 2010-2 (2010). 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).

Additionally, somewhat related, the San Diego County Bar Association’s Legal Ethics Committee dealt with a similar 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. San Diego Bar Ass'n on Legal Ethics, Op. 2011-2 (2011). 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, and it found that "friend-ing" is within "the subject of representation."

Model Rule 8.4 is by no means, the only ethical rule potentially implicated when an attorney seeks to friend a witness or opposing party. Model Rule 4.1 requires that in the course of representing a client that the lawyer not knowingly "make a false statement of material fact to a third person." The rule prohibits misrepresentations that "occur by partially true but misleading statements **or** omissions that are the equivalent of affirmative false statements." Since a material fact is one that could influence the listener, the act of omitting the purpose behind the friend request could prove to be a violation of Rule 4.1.

Further, Rule 4.2 provides an obstacle for this behavior. Rule 4.2 states that: "In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order." There is nothing to suggest that this rule does not apply to electronic communications. However, an argument can be made that "friend-ing" is merely accessing public information, which is not prohibited by the rule. For instance, if the opposing party runs a website, there is nothing prohibiting the opposing attorney from perusing that website.

Model Rule 4.3 seems to address the attorney "friend-ing" a third party witness. Model Rule 4.3 requires that a lawyer, in "dealing on behalf of a client [,]" ensure that an unrepresented party understands the lawyer's interests in communicating with that person and must proactively clarify misunderstandings that the party may hold. Here again, it is likely that an attorney or his agent would have a duty to inform that they are not merely a neutral third party.

Many view the “friend-ing” of an opposing party or witness to be similar to an undercover investigation. In both instances, the attorney is placed in a situation where “misrepresentation” is certainly more likely and perhaps key to obtaining information. The difference though is that in a criminal investigation the ends are thought to justify the means. Several states including Alabama, Alaska, Florida, Iowa, Virginia, and Wisconsin all have modified Rule 8.4 to create a prosecutorial exception. In these instances, it is ethically acceptable for an attorney to supervise an undercover operation. Outside of criminal investigations however, misrepresentation only seems excusable to prove civil rights violations and to investigate intellectual property infringement where the agent was merely observing normal business operations of the target.

Ultimately, as of yet, there is no hard answer to whether a lawyer may make friend requests or have his agents do so. It lies on the fringe of many of the rules. Generally, the account from which the request is sent must be valid and truthful. Further, 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.

Finally, and perhaps your best option, is that there is little to prevent a client from accessing others accounts. In other words, clients can friend individuals in an effort to conduct an investigation and then pass that information onto their attorney. An attorney can even passively use their client’s login credentials to access information that the client would ordinarily have access to. An attorney cannot direct their client to provide messages directly to opposing parties.

d. AUTHENTICATING THE DATA

A common objection to social media evidence is found under Fed. R. Evid. 901 that the material is not authentic.

In that case you can look to Fed. R. Evid. 904(b)(1), authentication through the testimony of a witness with knowledge that the evidence is what it is claimed to be. Electronic communications—including email, text message, or social media message can be authenticated through the testimony of the author (including participant in online chat) **or** 904(b)(4) permits authentication using circumstantial evidence, in conjunction with the appearance, contents, substance, internal patterns, or other distinctive characteristics.

Essentially, a witness testifies that an email, text message or social media message, originated from the known email address or social media page of the purported sender. Most courts will find this to be sufficient. For instance, in *United States v. Lanzon*, 639 F.3d 1293 (11th Cir. 2011), the court upheld the admission of transcripts of an instant messaging conversation an undercover agent had with a man attempting to solicit sex acts from a minor. 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.’”

However, some courts have been more stringent. For example, in *Griffin v. Maryland*, 419 Md. 343 (Md. Ct. App. 2011), a 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 that “the characteristics of the offered item itself, considered in the light of circumstances, afford authentication techniques in great variety, including 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.

Consistent with this is *People v. Lenihan*, where the mother of the defendant in a murder case downloaded photos from the government witness’s MySpace page four days after the shooting. 911 N.Y.S.2d 588 (N.Y. Sup. Ct. 2010). 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.

Likewise, in *Commonwealth v. Williams*, evidence was admitted from the defendant's MySpace account. 926 N.E.2d 1162 (Ma 2010). The prosecution was able to provide testimony from witnesses that inculpatory messages had been sent from the defendant's account. However, the Massachusetts Supreme Court found the trial court's admission of the evidence improper, because there had been no showing that only the defendant had access to the account. The court noted that just because a person received a phone call from a person claiming to be person A that did not actually mean that the person they spoke with was person A.

When it comes to admission of social media evidence, it appears that the key issue for the court is a fear of fabrication. While courts have struggled with this, some have begun to consider this a factual issue for the jury. In *People v. Clevestine*, another internet sexual assault case, the state presented testimony from a computer forensic analyst and a legal compliance officer from MySpace. 68 A.D.3d 1448 (N.Y. App. Div. 2009). 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."

With regard to email, some courts will require authentication from the sender, some from the recipient, and some will accept authentication from either. For instance, in *Network Alliance Group L.L.C. v. Cable & Wireless USA, Inc.*, inconsistencies within the alleged e-mail correspondence suggested that the correspondence was not authentic. No. CIV 02-644DWFAJB, 2002 WL 1205734, at *1 & n.2 (D. Minn. May 31, 2002). The date stamp for one of the email messages listed a date well into the future and an incorrect day of the week for that date.

Situations like *Network Alliance*, where all facts surrounding a correspondence are disputed, have led to alternative methods of authenticating ESI. One of these approaches has been to take judicial notice of other commonly known characteristics of computers. Check local authority as some courts interpret authentication requirements tougher than others and some will simply not accept it if another more traditional form is readily available.

To summarize, there are several methods of authentication for social media evidence. 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, as was done in *Clevenstine* under 901(b)(3) or maybe even 901(b)(9). Some have also used Fed. R. Evid. 901(b)(4) Distinctive Circumstances or Characteristics, which parallels the initial reasoning applied by the lower court in *Griffin*. 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.

e. CAN PRINT-OUTS OF MESSAGES BE ADMITTED? IN WHAT FORM TO SUBMIT THE DATA

Authentication of ESI typically involves two concerns. The first, and often the biggest concern for the court, is the identity of the alleged declarant discussed above. Also though, one must show that the proffered evidence of the alleged communication is an accurate representation of what was posted. In the 1960's courts were somewhat skeptical of computer printouts. Indeed, 1981 ALR suggested that when introducing computerized business records the foundation should include: (1) the reliability of the computer equipment used to keep the records and produce the printout; (2) the manner in which the basic data was initially entered into the computerized record-keeping system; (3) the entrance of the data in the regular course of business; (4) the entrance of the data within a reasonable time after the events recorded by persons having personal knowledge of the events; (5) the measures taken to insure the accuracy of the data as entered; (6) the

method of storing the data and the precautions taken to prevent its loss while in storage; (7) the reliability of the computer programs used to process the data; (8) the measures taken to verify the accuracy of the programs; and (9) the time and mode of preparation of the printout.

Recently, however, courts have not had great difficulty in accepting that a print out or screen shot is an accurate representation of various online communications. For example, in *United States v. Catrabran*, 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). Increasingly, the only bar to the admission of ESI is finding the applicable hearsay exception.

With regard to email, printouts typically contain the same identifiable information that is found in the email itself. The email address may incorporate the target’s name, the signature block may be unique to the sender, and the conversation may detail characteristics unique to the defendant. Typically, having a witness testify as to the whether the printout is a fair and accurate depiction of the email, highlighting various identifiable characteristics is enough for admission.

Web pages, instant messaging, and chat rooms have been handled similarly. In *Firehouse Restaurant Group, Inc. v. Scurmont LLC*, the court considered the authenticity of several printouts from various websites in a trademark dispute. C/A No. 4:09-cv-00618-RBH, 2011 WL 3555704 (D. S.C. Aug. 11, 2011). The plaintiff asserted that the printouts 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, *United States v. Tank*, 200 F.3d 627, 630–31 (9th Cir. 2000) found that chat room

transcripts and printouts could be authenticated by the testimony of one of the participants in the online chat.

Printouts of social media have been a little bit tougher for courts to handle. Similar to online chat rooms, individuals create a user id under a pseudonym or nickname. This, particularly in the realm of social media, has created authentication issues. However, most of these again revolve around the identity of the sender, not the accuracy of a computer printout or screen shot. Do not forget that the opposing party may even be willing to stipulate to the authenticity of the social media and the printouts.

In *LaLonde v. LaLonde*, the Court of Appeals of Kentucky considered pictures posted on Facebook when deciding a child custody case. No. 2009-CA-002279-MR, 2011 WL 832465 (Ky. Ct. App. Feb. 25, 2011). The husband sought to introduce photos from Facebook, to show his wife's alcoholism. The wife argued 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. There is nothing that requires her permission when she was ‘tagged’ or identified as a person in those pictures.” Accordingly, the wife's testimony that she was the person depicted in the photographs and that the photographs accurately reflected that she was drinking alcohol, was sufficient to meet the standard of authentication.

Ultimately, social media evidence, electronic evidence, and all forms of evidence are subject to the possibility of alteration. The use of computer printouts for ESI has largely become widely accepted and your greatest concern should be proving authorship of any alleged communication.

f. THE LATEST COURT OPINIONS

The previously mentioned *Crispin v. Christian Audigier, Inc.*, is the most recent and only major case to have applied the Electronic Stored Communications Act to Facebook. There the court quashed the portions of subpoena that applied to communications in the parts of the profile that the user had selected as private. 717 F.

Supp. 2d 965 (C.D. Cal. 2010). The court was even willing to consider wall posts as protected information because one of the many purposes of the user may have been backup storage for her photos and writings. In other words, Facebook may have been operating as an RCS for the user. The court remanded the matter to determine the privacy settings the plaintiff employed on her Facebook page.

Other courts have in large part ignored the SCA and held the entire profile discoverable. In *Romano v. Steelcase*, the 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. 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010). 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.

Similar to *Romano*, the court in *Ledbetter v. Wal-Mart Stores, Inc.*, No. 06-cv-01958-WYD-MJW, 2009 WL 1067018, at *1 (D. Colo. Apr. 21, 2009), refused to quash Wal-Mart's subpoenas aimed at the plaintiff's social media profiles. The subpoenas sought all communications, including private blog entries, but in this personal injury suit the court concluded the subpoenas were "reasonably calculated to lead to the discovery of admissible evidence as is relevant to the issues in this case." *Id.* at *2.

Most courts thus far seem to settle the issue of discoverability on relevance, although the courts after *Crispin* may consider protection under the SCA. Authentication often rests on the ability to show authorship, although some courts are more lenient only requiring an applicable exception to hearsay.

III. SMARTPHONE/TABLET DISCOVERY

a. CAN YOU TAKE THE OPPOSING SPOUSE'S SMARTPHONE/TABLET FOR EVIDENCE

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).

Also beware, a few states will allow a Guardian ad Litem to listen to recorded conversations caught in violation of the Federal or state Wiretapping statutes. Although the recordings cannot be admitted into evidence, they may prove influential. For an example of this see *In re Marriage of Karonis*, 693 N.E.2d 1282 (Ill. App. Ct. 1988).

The most common application for cell phones in a divorce matter is to subpoena the carrier for itemized billing. This is 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. With further regard to the discovery of emails on smartphones, subpoenaing internet service providers will typically only generate the sender and recipient of a message. ISP's like cell phone providers often delete this information quickly. Outside of intercepting telephone conversations or voicemails smart phone data and tablets akin to a computer. See cases listed above in Part I (e).

Ultimately, clients often recognize that their spouse's behavior is under the microscope in a dissolution proceeding, but frequently fail to realize that same microscope is looking at them as well. A general rule of thumb is: if you do not have an ownership interest in the device, you do not have access to it, although, there are exceptions. More often than not, the best method of acquiring ESI from computers, tablets, and smart phones is through formal discovery. At a preliminary hearing ask for an injunction with regard to the deletion of various ESI sources and be prepared to subpoena potential sources of ESI.

b. RETRIEVAL OPTIONS FOR DELETED DATA

If you know that you have deleted relevant data, or you suspect the opposing party has done so, you have several options. First, if you own the device or account in question, you may be able to personally contact the provider without the need for a subpoena. 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, but you can attempt to gain consent from the opposing party.

Additionally, and likely your best bet is to hire a computer forensic expert. As discussed above, they may be able to uncover data believed to have been deleted long ago, or they may uncover data that was merely hidden from the common user. They may also be able to provide insight as to the meaning of metadata discovered on various files.

Finally, do not underestimate the ability to locate information elsewhere. People often sync any number of devices to each other. For this reason, a home computer may be a better source of information than you might initially suspect. Also, beyond other devices consider other people. In the process of jubilant celebration or angry venting, people often write, forward, or post about their recent endeavors. You might discover that the photos you forwarded to a friend are still on their device or that text messages to a mistress deleted from the husband's phone are still located on the mistress' devices. In today's day and age, it is rare that a piece of ESI is truly gone forever. Just be prepared for any additional authentication issues you may have when locating data from an alternative source.

c. IN WHAT FORM CAN TEXTS BE ADMITTED INTO EVIDENCE?

Similar to a computer printout of a software application or website, a print out of a text message will typically be sufficient. Some phones will allow you to transfer text files onto a computer and this can be accomplished with relative ease. Many individuals will also have an automatic back-up system located on their computer or in a cloud. In other cases, you can always take a photograph of the text message. Many phones such as the iPhone, will simply let you snap a screen shot which can then be uploaded and printed. Of course, the device itself can also be used, but this results in the loss of its use

while it is being used as evidence. Sometimes, depending on the make and model of the phone, the messages may be stored on the SIM card and the card may simply be removed and preserved with a new one inserted for use.

In *State of Hawaii v. Espiritu*, the admissibility of text messages was addressed in the appeal of a criminal conviction for attempted second-degree murder. 176 P.3d 885 (Haw. 2008). Text messages from the petitioner relating to the murder were held admissible because, like e-mails, a text message is considered to be a “writing” under Fed. R. Evid. 1002. Since the complainant no longer had the cell phone from which the text messages were received and no other copies of the text messages existed, the 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.”

IV. INSTAGRAM, VINE, SNAPCHAT, AND OTHER PHOTO AND VIDEO SHARING APPS

a. EVIDENCE SPOILIATION: CAN YOU RETRIEVE DELETED CONTENT?

Snapchat is a photo messaging, social media tool. Unlike other services, Snapchat seeks to provide impermanence. Users can share photos, record video, and add text for distribution to one or more recipients. Those shares are set to self-destruct or disappear up to 10 seconds after sharing. The app also includes features which require the recipient to prove they are using their phone. Notice is also provided to the sender of any users taking a screenshot. Snapchat is billed as providing two-way communication of photos and videos without leaving any incriminating evidence. Recently, there have been weaknesses revealed as to Snap-chat's claims of destruction. Their own privacy policy acknowledges: “Although we attempt to delete image data as soon as possible after the message is received and opened by the recipient ... we cannot guarantee that the message

contents will be deleted in every case ... Messages, therefore, are sent at the risk of the user.”

There are additional methods of preserving videos. For example, recipients can simply take a screenshot of the message, although this will notify the sender. Alternatively, recipients can take a picture of their phone, thereby circumventing the screenshot notification. Even then, a more complicated approach exists. Snapchat saves [videos] on the phone's local memory, on some phone models, which you can then recall by installing a file browser, and plugging the phone into a computer. You then search through the file browser, copy and save the content to a computer, and you're done. Indeed a May 9, 2013, Forbes article detailed that one forensic firm was able to pull many Snapchat photos from a phone long after they were supposedly deleted. Also, Snapchat has stated that if a file is not viewed it will remain on their servers for 30 days.

Instagram, now owned by Facebook, is another online photo-sharing and social networking service that enables its users to take a picture, apply a digital filter to it and share it on a variety of social networking services, including Facebook. Unlike Snapchat, however, the data is stored on Facebook's servers and is not automatically deleted a few seconds after viewing. Access to the device should provide access, and materials that are deleted are likely recoverable by a forensic analyst. Further, one could subpoena Instagram, but one would likely face the same challenges one experiences when subpoenaing Facebook.

Vine is also a videosharing mechanism. Vine is a mobile app owned by Twitter that enables its users to create and post 6.5 second video clips. The service allows videos to be shared or embedded on social networking services such as Twitter and Facebook. Seemingly, more similar to Instagram than Snapchat, it would appear as though videos could be recovered both from the device and Vine's servers; although Twitter's website says deletion is permanent within a few minutes. Since the videos may be embedded in websites, the information might be recoverable from a personal computer by examining browser history as well. In addition, Twitter's website seems slightly more amendable to compliance with civil subpoenas than say Facebook. The website does mention that

different types of data are retained on its servers for different amounts of time, thus again success depends upon rapidly securing the content.

b. GETTING THE DATA ADMITTED INTO EVIDENCE

This will depend upon how you received the data. For instance, Twitter's website (in reference to Twitter accounts or Vine) states that its data production comes in electronic format capable of viewing by common word processors such as Microsoft Word. Additionally, the website mentions that its records are self-authenticating and come with an electronic signature to ensure the integrity at the time of production. A declaration will be provided upon request.

Even if subpoenaing one of these providers or a social media outlet in general, it can be wise to seek consent first. The SCA allows the provider to provide the user's records with "the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service ...". A well drafted consent form should include the account holder or user's name, any user id or known screen name, along with the person's date of birth and address, including email address, as many providers require this information anyway. The consent should also include a detailed description of what information is targeted and a notarized signature of the consenting party.

If you are not receiving the data as part of a response to a subpoena, you have other options. You could take printouts of the video similar to photos taken from social media websites. However, beware that most of these video sharing outlets allow for pseudonyms and nickname, which makes the biggest challenge the issue of who uploaded the video. Additionally, these could be played in court from the sender's or recipient's video sharing account with corroborative testimony. This may be the better option depending on whether a still image can capture the behavior you are attempting to prove. Be prepared with your Fed. R. Evid. 101 and 904(b) methods of authentication and applicable exceptions to hearsay.

V. DISPUTING SOCIAL MEDIA AND SMARTPHONE DISCOVERY

a. CONTESTING THE VERACITY OF THE ONLINE INFORMATION

Often the best place to begin your challenge of ESI and social media evidence, in particular, is on authenticity. Every piece of evidence that is admitted must meet a threshold standard of authenticity under F.R.E. 901. It does not need to be proven that the object is what it is purported to be, only that a reasonable juror could find it to be what it is purported to be. Federal Rule of Evidence 104(b) makes this a preliminary determination for the judge. In other words, the judge is the gatekeeper.

Authentication of social media often devolves into two categories. The first is the identity of the alleged declarant and the second is whether the offered evidence is an accurate representation of the material to be found online. As discussed previously, courts are increasingly finding a printout of a social media website to be a fair and accurate depiction of a website, but it may still be worth a try if you can point out discrepancies between the current site and the print out.

Calling into question the identity of the social media user has been successful. The first step, however, is to consider how your opponent will seek to authenticate the information. If the opponent is likely to utilize F.R.E. 901(b), by having a witness testify as to the origins of the communication, you can attempt to attack their credibility. If the opposing party is likely to attempt authentication of ESI through distinctive characteristics of the material, attempt to show that the characteristics are not so distinctive. This is essentially what happened as *Griffin v. Maryland*, 419 Md. 343 (Md. Ct. App. 2011), moved up the Maryland court system. Commonly, a successful argument is that others had access to the computer, phone, or media outlet. Many courts are cognizant that photos and documents may be altered and online accounts hacked. Consequently, this can be successful even if the other side is attempting to use an expert to show the trustworthiness of the process in which the alleged records are made. Finally, and if finances allow, you might be able to show another user posted the alleged content through metadata.

b. CONTESTING THE PROCESS OF OBTAINING THE INFORMATION

There are several possible objections a party may make with regard to the manner in which ESI discovery is conducted. The first rationale, and perhaps the rationale the

courts were initially most willing to accept, was that a discovery request was overly burdensome or costly under Fed. R. Civ. P. 26(b)(2)(B). Generally speaking, the cost of allowable E-Discovery will vary directly with the amount in controversy. According to the Comments associated with Fed. R. Civ. P. 26(b)(2)(B) in accessing discoverability the court should consider: (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources. Many of these factors are explicitly considered under Fed. R. Civ. P. 26(b)(2)(C), which authorizes a protective order to limit discovery.

Rule 26(b)(2)(C) provides:

When Required. On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:

- (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;
- (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or
- (iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

Be mindful, though, that this is a Federal Rule of Evidence, while adopted in most jurisdictions the particularities of E-Discovery may differ in your jurisdiction.

Also, even if the judge does not find that the material is too burdensome or costly, the judge does have the authority to shift the burden of discovery related costs.

Ordinarily, the producing party bears the burden of the associated costs, but instances where a party requests that documents be provided in a format different from which they are usually kept, may be sufficient to justify expense shifting. Other factors such as whether the information is available from other sources, such as depositions, interrogatories, requests for admission, or other discovery devices; each party's respective resources; the nature of the issue being litigated; and, each party's ability to control costs.

Further, one can object that the discovery request is likely to produce privileged material. Fed. R. Civ. P. 26(b)(5)(B) is essentially a clawback provision. It provides that if information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The producing party must preserve the information until the claim is resolved.

Finally, and often related to burden and cost, one can object that discovery of, in this case, social media evidence is not relevant to the matter at hand. In order for any evidence to be admitted, it must as a threshold matter be relevant under F.R.E. 401. Depending upon what issue is being contested, your client's social media use may provide no insight as to finances or child care habits. Further, even if there is evidence to be found, perhaps the purpose for which the materials are being sought is not relevant. Take infidelity for example, in most no-fault jurisdictions, evidence of marital indiscretion so long as it is not wasting marital resources is irrelevant.

VI. ARE THE EX'S DISPARAGING REMARKS IN SOCIAL MEDIA PROTECTED UNDER THE FIRST AMENDMENT

In 2010, Steve Nash, a basketball player for the Los Angeles Lakers, filed for dissolution of his marriage to Alejandra Nash. *Nash v. Nash*, 307 P.3d 40 (Az. Ct. App. 2013). The parties were able to resolve custody and parenting time with their two

young children through a joint agreement, but the matter went to trial on the issue of child support. On the day the trial court issued its decree, Mrs. Nash “tweeted” several disparaging remarks pertaining to Mr. Nash.

Mrs. Nash then took several issues up on appeal. Following her tweet on the day of the decree, Mr. Nash had sought a court order prohibiting such conduct based upon their joint custody agreement which contained the following language:

All communications between the parents shall be respectful. The parents agree that neither parent shall disparage the other party to the children, and that each parent shall model respect for the other parent in their interactions with the children. Neither parent shall do or say anything to the children that would negatively impact the child's opinion or respect for the other parent.

Mr. Nash approached the parenting coordinator with the content of the social media posting and the text of their parenting agreement. The parenting coordinator then wrote to the court:

Mother is cautioned against communicating about Father in a negative and pejorative way, especially using social media. Most recently, it has been brought to the [Parenting Coordinator]'s attention that Mother has “tweeted” about Father in an unflattering way. Mother is entitled to her own feelings about Father. However, using social media to tell the world how she views Father is insensitive to Father's role in relationship to his children. If parents of the children's friends, for example, were to view Mother's comments, it could negatively influence the parents and their children regarding the Nash children. The [Parenting Coordinator]'s concern is the collateral effect to the children. Mother must stop these activities.

In response, the court issued the following order:

With respect to the allegations [about the tweet], the parties are reminded that the [joint custody agreement] is an Order of the Court. Violation of the terms of the [joint custody agreement] is not solely a matter resolved by the Parenting Coordinator, but is enforceable by the Court. The life span of social media is indefinite. Distribution of social media postings cannot be effectively controlled or contained. Disparaging comments made by either party regarding the other party violates the [joint custody agreement] and is likely, over time, to be viewed by the minor children. The parties are reminded that such conduct is prohibited.

Mrs. Nash then challenged the order on appeal as violating her First Amendment right to free speech. The court began its analysis by classifying the order prohibiting “disparaging comments” as a prior restraint on speech. In order to justify prior restraint, the most serious infringement on the First Amendment, the order had to serve a compelling government interest and be the least restrictive means for accomplishing that end.

In general, the court found the agreement itself, prohibiting the parents from disparaging in front of the children, to be non-problematic. Similar orders had been upheld in *In re Marriage of Hartmann*, 185 Cal.App.4th 1247 (Cal. Ct. App. 2010) and *In re Marriage of Olson*, 850 P.2d 527 (Wa. Ct. App. 1993). However, orders prohibiting communications with third parties were a different matter. Order of this variety had been previously struck down in *In re K.D.*, 929 N.E.2d 863 (Ind. Ct. App. 2010) and *In re T.T.*, 779 N.W.2d 602 (Neb. Ct. App. 2009).

The court acknowledged that the trial court’s order went beyond the explicit language of the joint agreement. The court cited *Adams v. Tersillo*, 245 A.D.2d 446, 447 (N.Y. App. Div. 1997), where an order was limited to comments made in the presence of the children or those made in the presence of those who have contact with the children. While here the underlying joint agreement did not speak to third party communications, the court took notice of the unique circumstances presented here. Mr. Nash’s high profile

career as an NBA basketball player made it more likely that such remarks would find their way back to the children. The court found the prohibition of public remarks to be within the spirit of the joint agreement.

Mrs. Nash though did not entirely fail in her First Amendment arguments. Mrs. Nash also challenged an order which sealed the “documents, records, and transcripts” of the court. In addition, the order also prohibited discussing the outcome of the proceeding or any of the sealed documents. Again, the court viewed this as a prior restraint on speech. And here as well, Mr. Nash attempted to rely on the joint agreement made prior to trial.

This time, however, the court did not find a compelling interest to justify such a broad prohibition. Such a broad order was not a “logical extension” of the joint agreement. The order was prohibiting speech concerning a public proceeding and the trial court had not made the specific findings required for such an order. Unlike the prohibition on disparaging remarks which was warranted by a concern for the children, there was nothing in the court’s file which would threaten the best interests of the children.

The ultimate takeaway from *Nash v. Nash* is that it is an exceptional case. The success of Mr. Nash’s was predicated upon their existing joint agreement. Without the language found in the joint agreement, it is unlikely such an order would have been granted in the first place. This seems to be showcased by the second point on appeal regarding the First Amendment. In this circumstance, the court not guided by any specific provisions in the joint agreement, struck down the prohibition on speech. Moreover, the court took specific notice of Mr. Nash’s celebrity status. It seems entirely possible that even with the agreement, the court would have struck down the order pertaining to social media had the Nash’s not been such a high profile family. Finally, the court may have been influenced by the content of Mrs. Nash’s tweets. The court was unwilling to repeat them in its opinion, which gives rise to the inference that they may have been particularly inappropriate and represented a potentially serious ongoing problem.

Moving forward, it is likely that the cases cited by the court will continue to mark the landscape for divorcing parties and the First Amendment. A court may easily grant an order preventing disparaging remarks between the parties. An order prohibiting communications with third parties will remain highly suspect. If you are seeking to prohibit third party communications, your best bet is to attempt some form of joint agreement which, best case scenario, explicitly addresses the situation, or like the agreement in *Nash*, does so implicitly in a scenario where publicity is likely to harm the children involved.