SOCIAL AND ELECTRONIC MEDIA AND THE LAW


SOCIAL
MEDIA
BLOG
SMS
BLOG
SMS

SOCIAL MEDIA
YOU CANNOT IGNORE IT

- **91 percent of today's online adults use social media** regularly, and "[s]social networking continues to reign as the top online activity."
- Social media use in the United States alone has increased by **356 percent** since 2006. Currently, 52 percent of Americans have at least one social media profile more than one billion people use Facebook actively each month, and **Twitter has over 140 million active users posting 340 million Tweets a day**.
- Every minute, social media users create massive amounts of data: Facebook users share 684,478 pieces of content; Tumblr blog owners publish 27,778 new posts; YouTube users upload 48 hours of new video; Foursquare users perform 2,083 check-ins; Flickr users add 3,125 new photos, and Instagram users share 3,600 new photos. In addition, there are hundreds of other social networking websites, each catering to a different demographic.
- The myriad and continually changing ways to share information via social media has resulted in a digital goldmine of potential evidence: profiles, lists of friends, group memberships, messages, chat logs, Tweets, photos, videos, tags, GPS locations, check-ins, login timetables and more.

- The information available from social media providers is staggering. When a phone company responds to a government subpoena or search warrant, it may provide call or message logs. In contrast, when a social media company such as Facebook responds to a government subpoena it provides the user's profile, wall posts, photos uploaded by the user, photos in which the user was tagged, a comprehensive list of the user's friends with their Facebook IDs, and a long table of login and IP data.

- Moreover, with the advent of location-based services offered by social media companies like Facebook, Twitter, and FourSquare, precise location information will be increasingly maintained in the ordinary course of business and subject to the same subpoenas and search warrants. Not surprisingly, each social media subpoena can yield admissions or incriminating photos, among other evidence.

BLOGS

BLOGS

- A blog (a contraction of the words web log) is a discussion or informational site published on the Web and consisting of discrete entries ("posts") typically displayed in reverse chronological order (the most recent post appears first).
- Until 2009 blogs were usually the work of a single individual, occasionally of a small group, and often covered a single subject

BLOGS

- **How Do I Find Someone's Blog Site?**
- To find a person's blog, you can either do a search for the blog's name or their name (if their name is attached to the blog).
- You can also ask the person for their blog's URL address so that you can type it in to a browser; from there you can save the site for future reference.

BLOG SITES

- Wordpress (http://wordpress.com) is at the top of the list for people who run a web site and want to incorporate blogging or who want to do "multi-user blogging".
- Blogger/Blogspot (http://blogger.com) is at the top of the list for people who would rather have a service control the primary web site functions and provide automated tools/features (i.e. developer-hosted blogging). Wordpress can also be used as a developer host. Blogger is well known for its ease of use.
- Other popular blog services:
- Livejournal (http://livejournal.com), Vox (http://vox.com), Typepad (http://typepad.com), Travelpod (http://www.travelpod.com/), Tumblr (http://www.tumblr.com/), Posterous (http://www.posterous.com//)

FACEBOOK

FACEBOOK

- **Facebook Friend Finder:** Enables you to scan the e-mail addresses in your e-mail address book to find whether those people are already on Facebook.
- **Share your thoughts**
- **Share your pictures – tagging and untagging**

FACEBOOK

- Privacy settings; The user may change privacy settings to restrict access by blocking others from “subscribing” to one’s updates from changing other permissions.
- However, no privacy setting will completely restrict a party in a lawsuit form access to published Facebook content.
- Deleting from Facebook is not easy.

FACEBOOK

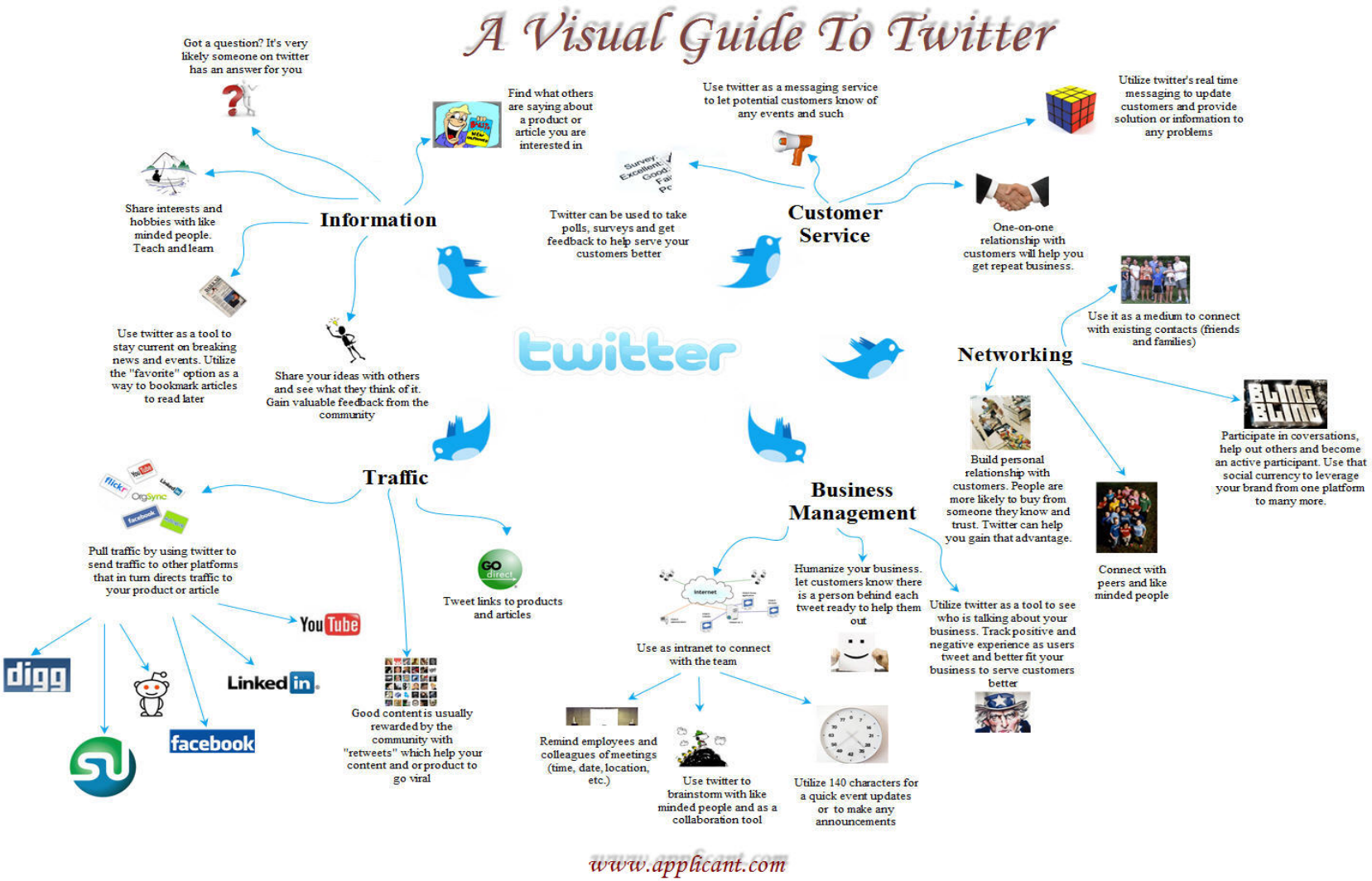
- BUT
- The social network announced October 10, 2013 that it is removing a privacy setting that lets you decide whether or not you want your profile to appear when people search for you by name.
- The setting, called "Who can look up your Timeline by name," was already removed last year for people who weren't using it. Facebook said there is a "small percentage" of people still using the setting; they will see reminders about its removal in the coming weeks.
- As a result, all Facebook users will be searchable when someone types their name into the search bar.

FACEBOOK

- Facebook's Privacy Policy
- Responding to legal requests and preventing harm

- We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if **we** have a good faith belief that the law requires us to do so. . .
- We may also access, preserve and share information when **we** have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; and to prevent death or imminent bodily harm.
- Information we receive about you, including financial transaction data related to purchases made with Facebook Credits, may be accessed, processed and retained for an extended period of time when it is the subject of a legal request or obligation, governmental investigation, or investigations concerning possible violations of our terms or policies, or otherwise to prevent harm. We also may retain information from accounts disabled for violations of our terms for at least a year to prevent repeat abuse or other violations of our terms. .

TWITTER


A Visual Guide To Twitter
Got a question? It's very likely someone on twitter has an answer for you
Find what others are saying about a product or article you are interested in
Share interests and hobbies with like minded people. Teach and learn
Information
Use twitter as a tool to stay current on breaking news and events. Utilize the "favorite" option as a way to bookmark articles to read later
Share your ideas with others and see what they think of it. Gain valuable feedback from the community
Use twitter as a messaging service to let potential customers know of any events and such
Utilize twitter's real time messaging to update customers and provide solution or information to any problems
Twitter can be used to take polls, surveys and get feedback to help serve your customers better
Customer Service
One-on-one relationship with customers will help you get repeat business.
twitter
Networking
Use it as a medium to connect with existing contacts (friends and families)
Participate in coversations, help out others and become an active participant. Use that social currency to leverage your brand from one platform to many more.
Build personal relationship with customers. People are more likely to buy from someone they know and trust. Twitter can help you gain that advantage.
Connect with peers and like minded people
Traffic
Pull traffic by using twitter to send traffic to other platforms that in turn directs traffic to your product or article
digg
YouTube
LinkedIn
facebook
Tweet links to products and articles
Good content is usually rewarded by the community with "retweets" which help your content and or product to go viral
Business Management
Use as intranet to connect with the team
Humanize your business. let customers know there is a person behind each tweet ready to help them out
Utilize twitter as a tool to see who is talking about your business. Track positive and negative experience as users tweet and better fit your business to serve customers better
Remind employees and colleagues of meetings (time, date, location, etc.)
Use twitter to brainstorm with like minded people and as a collaboration tool
Utilize 140 characters for a quick event updates or to make any announcements
www.applicant.com

TWITTER

- Twitter is an online social networking and microblogging service that enables users to send and read "tweets", which are text messages limited to 140 characters. Registered users can read and post tweets but unregistered users can only read them.

Finding people on Twitter

- How to find people by name:
- (1) Type the person's name into the search box at the top of your Twitter homepage.
- (2) Results for your search will show up under the People tab on the search results page.
- (3) You can also search by typing the person's name into the search box on the Connect page.
- Look up whomever you wish to follow via the Twitter search bar. Enter a name, then click the magnifying glass to search. A row of options will appear, allowing you to specify your search by tweet, tweets with links, tweets near you, and people. For the most efficient results, click "People".

Finding people on Twitter

- Name, Profile, Location and Tweets
- 1) Searching for Twitter users based on their name
- site:twitter.com intitle:”james* * on twitter”
- site:twitter.com intitle:”peter* * on twitter”
- You can also search for a person’s full name, for example;
- site:twitter.com intitle:”stuart laing * on twitter”
- Just change the name in the search to suit your own needs.
- 2) Searching for Twitter users on the words used their bio profile
- site:twitter.com intitle:”on twitter” “bio* * sport”
- This will provide you with a long list of people who have used the word sport in their Twitter bio. Again, just alter the search term to suit your own needs.
- 3) Searching for Twitter users based on the location in their profile
- site:twitter.com intitle:”on twitter” “location florida”
- Google will return a list of Twitter users based in Florida.
- It’s also possible to combine these search factors, for example, if you want to search for Twitter users based on their location and the words used in their profile, use this search formula;
- site:twitter.com intitle:”on twitter” “bio* * pr” “location florida”
- This will return a list of Twitter users based in Florida who have PR in their bio.
- 4) Seaching for Twitter users based on the words that appear in their tweets
- site:twitter.com/*/statuses/* “golf”
- This will return a list of all the Twitter messages containing the word Golf that have been indexed by Google.
- If you prefer to use Twitter specific search tools, here are a few of the best options;
- Twitter Search Is the main Twitter search engine
- TweepSearch Allows you to search for people according to the words that appear in their Twitter profile

INSTAGRAM

Instagram

INSTAGRAM

- Instagram is an online photo-sharing, video-sharing and social networking service that enables its users to take pictures and videos, apply digital filters to them, and share them on a variety of social networking services, such as Facebook, Twitter, Tumblr and Flickr. ...

FLICKR

- Flickr is an image hosting and video hosting website, and web services suite that was created in 2004 and acquired by Yahoo! in 2005.
- In addition to being a popular website for users to share and embed personal photographs, and effectively an online community, the service is widely used by photo researchers and by bloggers to host images that they embed in blogs and social media.
- In March 2013 Flickr had a total of 87 million registered members and more than 3.5 million new images uploaded daily.

TUMBLER

- Yahoo's purchased Tumbler for $1.1 billion in 2013
- **Tumblr**, is a microblogging platform. A microblog differs from a traditional blog in that its content is typically smaller in both actual and aggregated file size. Microblogs "allow users to exchange small elements of content such as short sentences, individual images, or video links".
- The service allows users to post multimedia and other content to a short-form blog. Users can follow other users' blogs, as well as make their blogs private.
- As of October 1, 2013, Tumblr hosts over 139.4 million blogs.

SOCIAL MEDIA AND THE CIVIL CASE

- You can get to know your client maybe before he/she becomes your client.
- On intake ask for Facebook page name and Twitter account
- You prospective client surely looked you up on the internet
- Do research on your prospective commercial client- see what their website says and be prepared to determine if their claim or defense is inconsistent in some way based on what you learn about he company.
- For the Defendant- Learn all you can as soon as you can before postings begin to change.
- What about your expert? What has he or she been saying on social media

SOCIAL MEDIA AND THE CIVIL CASE

- FIRST ORDER OF BUSINESS: The Litigation Hold letter
- a legal hold (also known as a litigation hold, preservation order, suspension order, freeze notice, hold notice or hold order) is a process that an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated.
- The hold must also confirm that any applicable document destruction procedures or policies of an organization must be appropriately suspended. A legal hold communication should also explain the ramifications of failure to comply with its directives.
- From the moment that litigation is reasonably anticipated, a potential litigant must preserve all relevant materials including electronically stored data and social media content
- Posts on Social media are within the scope of “electronically stored information” under Fed. R. Civ. P. 34.

ETHICAL CONSIDERATIONS AND SOCIAL MEDIA

- NEW YORK STATE BAR ASSOCIATION
  Committee on Professional Ethics
- Opinion # 843 (09/10/2010)

- **Question**: May a lawyer view and access the Facebook or MySpace pages of a party other than his or her client in pending litigation in order to secure information about that party for use in the lawsuit, including impeachment material, if the lawyer does not "friend" the party and instead relies on public pages posted by the party that are accessible to all members in the network?
- **OPINION**

  Social networking services such as Facebook and MySpace allow users to create an online profile that may be accessed by other network members. Facebook and MySpace are examples of external social networks that are available to all web users. An external social network may be generic (like MySpace and Facebook) or may be formed around a specific profession or area of interest. Users are able to upload pictures and create profiles of themselves. Users may also link with other users, which is called "friending." Typically, these social networks have privacy controls that allow users to choose who can view their profiles or contact them; both users must confirm that they wish to "friend" before they are linked and can view one another's profiles. However, some social networking sites and/or users do not require pre-approval to gain access to member profile
- Here, in contrast, the Facebook and MySpace sites the lawyer wishes to view are accessible to all members of the network. New York's Rule 8.4 would not be implicated because the lawyer is not engaging in deception by accessing a public website that is available to anyone in the network, provided that the lawyer does not employ deception in any other way (including, for example, employing deception to become a member of the network). Obtaining information about a party available in the Facebook or MySpace profile is similar to obtaining information that is available in publicly accessible online or print media, or through a subscription research service such as Nexis or Factiva, and that is plainly permitted. Accordingly, we conclude that the lawyer may ethically view and access the Facebook and MySpace profiles of a party other than the lawyer's client in litigation as long as the party's profile is available to all members in the network and the lawyer neither "friends" the other party nor directs someone else to do so.

- **CONCLUSION**
- A lawyer who represents a client in a pending litigation, and who has access to the Facebook or MySpace network used by another party in litigation, may access and review the public social network pages of that party to search for potential impeachment material. As long as the lawyer does not "friend" the other party or direct a third person to do so, accessing the social network pages of the party will not violate Rule 8.4 (prohibiting deceptive or misleading conduct), Rule 4.1 (prohibiting false statements of fact or law), or Rule 5.3(b)(1) (imposing responsibility on lawyers for unethical conduct by nonlawyers acting at their direction).

ETHICAL CONSIDERATIONS AND SOCIAL MEDIA

- **New York City Bar Formal Opinion 2010-2: OBTAINING EVIDENCE FROM SOCIAL NETWORKING WEBSITES**
- **QUESTION:** May a lawyer, either directly or through an agent, contact an unrepresented person through a social networking website and request permission to access her web page to obtain information for use in litigation?

- A lawyer may not use deception to access information from a social networking webpage. Rather, a lawyer should rely on the informal and formal discovery procedures sanctioned by the ethical rules and case law to obtain relevant evidence.

ATTORNEY -CLIENT COMMUNICATIONS AND SOCIAL MEDIA

- Social media provides the potential for both client and attorney to waive work-product doctrine protection and attorney-client privilege by publicly disclosing confidential information.

- Voluntary disclosure of the content of a privileged attorney communication constitutes waiver of the privilege as to all other such communications on the same subject. Generally, to constitute a waiver, the disclosure must be voluntary and inconsistent with the confidential nature of the attorney-client relationship and must be made to "unnecessary third parties."

ATTORNEY -CLIENT COMMUNICATIONS AND SOCIAL MEDIA

- In the YouTube "dancing baby" case, the court held that the plaintiff waived her attorney-client privilege by virtue of posts on her blog, gmail chat, and emails discussing those communications. Lenz v. Universal Music Corp., 2010 U.S. Dist. LEXIS 119271 (N.D. Cal. Oct. 22, 2010).
- In *Kintera, Inc. v. Convio, Inc*., 219 F.R.D. 503 (S.D. Cal. 2003), Kintera sued its competitor Convio for copyright infringement and misappropriation of trade secrets after Convio allegedly obtained a CD Rom belonging to Kintera containing proprietary and confidential computer program codes relevant to both companies' Internet-based marketing and fundraising services. For commercial reasons, Kintera discussed the alleged misappropriation of trade secrets on its company website and noted that it had obtained signed affidavits under penalty of perjury from Convio employees. During discovery, Kintera tried to withhold the affidavits from Convio pursuant to the work-product doctrine, but based on the disclosures of the affidavits on Kintera's website, the court rejected Kintera's objections and ordered that Kintera produce the witness statements contained in the affidavits.

ATTORNEY -CLIENT COMMUNICATIONS AND SOCIAL MEDIA

- In Stern v. O'Quinn, 253 F.R.D. 663 (S.D. Fla. 2008), Howard K. Stern, the attorney and friend of Anna Nicole Smith, filed a defamation suit against a firm after the firm allegedly made defamatory statements about Mr. Stern to the media while representing Ms. Smith's mother, Virgie Arthur. Concurrently, a book entitled Blond Ambition: The Untold Story Behind Anna Nicole Smith's Death was published and accused Mr. Stern of numerous criminal acts.
- An investigator for the book discussed the results of her investigation with the author and also made numerous statements in on-line chat rooms regarding her investigative progress, including strategy, to have Mr. Stern prosecuted, as well as conversations she had with Ms. Arthur. During discovery, Mr. Stern sought documents from the firm that supported the statements made by the firm to the media. The discovery requests sought to determine the firm's efforts in investigating whether the statements it made about Mr. Stern were true or false, including the statements made by the investigator for the Blond Ambition book.
- The firm claimed that the investigation for the book was protected by the work-product doctrine, but the court rejected the argument because the contents of the investigation were published in chat rooms and to the author of the book. Accordingly, the court required the production of all postings in the chat rooms and all documents and statements provided to the author of the book.

ATTORNEY -CLIENT COMMUNICATIONS AND SOCIAL MEDIA

- You may consider a social media warning statement in an engagement letter. A sample notice might read as follows:

- We strongly encourage you to refrain from participating in social media (Facebook, Twitter, Tumblr, Flickr, Skype, and the like) during the course of representation. Information found on social media websites is not private, can be discoverable, and if used as evidence may be potentially damaging to your interests. Understand that information shared with others be it verbally; in writing via email, text message or letter; or even posted online could result in a waiver of the attorney client privilege were that information to relate in any way to the legal matter that we are handling for you. In addition, you should not delete or remove information from any social media website as that could be considered destruction of evidence, spoliation of evidence, or obstruction of justice.

- We also advise you to refrain from communicating with us on any device provided by your employer or any computer, smart phone, or other device that is shared with someone else. In addition when communicating with us, do not use your work email address or a shared email account. You should only use a private email account that is password protected and only accessed from your personal smart phone or computer. We reserve the right to withdraw as counsel if the above advice is not followed.

E-Mails and the Privilege: United States v. Finazzo

- Highlights the personal risk that an employee's use of a work email account to send or receive otherwise privileged and confidential communications—for example, with a spouse, personal lawyer, or doctor—will be deemed a waiver of the applicable privilege. Finazzo reflects the recent trend of courts finding that the employee has no reasonable expectation of privacy in these circumstances, thereby vitiating any privilege.

- Finazzo involved a criminal prosecution, and ultimate conviction, of a former executive of clothing retailer Aéropostale. Christopher Finazzo was charged with participating in a kickback scheme in which he received a portion of the profits on Aéropostale's purchases from South Bay Apparel. The kickback scheme allegedly defrauded Aéropostale by depriving it of the ability to make informed and sound purchasing decisions, and by causing it to overpay for goods purchased from South Bay. The scheme was uncovered during an unrelated internal investigation. The investigating firm discovered an email to Finazzo from his personal trusts and estates attorney that had attached a list of Finazzo's assets for purposes of preparing a will. The schedule of assets showed that Finazzo was a co-owner of South Bay with Douglas Dey, and also co-owned several other companies with Dey, none of which had been disclosed to Aéropostale. Finazzo claimed that (i) he never consented to or encouraged his attorney to send privileged emails to his work account, (ii) he did not know the lawyer was going to send the email to his work account, (iii) he immediately forwarded it to his personal account and deleted it from his work account, and (iv) he instructed his lawyer not to send emails to his work account again.5 Finazzo therefore argued that the email was privileged and should not have been produced to the government by Aéropostale. He thus sought to have it excluded from evidence in his criminal trial.

- The District Court rejected Finazzo's motion in limine to exclude the email. The court first noted that Finazzo had the burden of proving that the email was privileged, including showing that it was made and maintained in confidence. In deciding the motion, the court applied a four-factor test first developed in In re Asia Global Crossing. Under this approach, the court evaluates: (1) whether the employer's policies permit or prohibit personal use; (2) whether the company monitors use of the employee's email; (3) whether third parties have a right of access; and (4) whether the company advised the employee or whether the employee was aware of the use and monitoring policies. As a result of this analysis, the court held that Finazzo had waived the attorney-client privilege over the email his lawyer sent to his work account.

- Specifically, although there was some dispute whether the policy in effect in 2006 when the email was sent prohibited all personal communications (the 2004 policy) or permitted limited personal use of the work email account (the 2007 policy), both policies warned employees that they "should have no expectation of privacy when using Company Systems." Moreover, between 2002 and 2006 Finazzo repeatedly had affirmed that he had read and was familiar with the company's Employee Handbook, which contained the policy on use of company technology systems. Even though there was no evidence that Aéropostale actually monitored employee emails, the court concluded that Finazzo's acknowledgement of the policies that permitted Aéropostale to review such emails defeated any claim that he had a reasonable expectation of privacy in emails sent from or received in his work email account.

E-Mails and the Privilege: United States v. Finazzo

- Unless company policy clearly provides that personal emails from a work account will be maintained in confidence and not monitored or reviewed by company personnel or third parties, an employee must seriously consider the very real risk that privilege will be waived before communicating with a personal lawyer from a work email account—whether about revising a will, matrimonial issues, civil litigation or potential regulatory or criminal investigations.
- Except for the most innocuous of scheduling emails, the convenience of using a work email account typically will not justify the risk of a privilege waiver.
- Thus, the best practice for the most sensitive of confidential, privileged discussions often remains a telephone conversation or face-to-face meeting. Indeed, while any privilege waiver should be limited to the actual emails sent or received in the work account, it is possible that frequent use of a work account could lead to claims of a subject matter waiver for all communications with counsel on a particular topic.
- Finazzo also cautions that one must exercise care in giving a work email address to lawyers or other with whom the employee may communicate in confidence on non-business related matters, unless clear instructions are given as to what emails may be sent to the work account.

FEDERAL STORED COMMUNICATIONS ACT

- Courts have held that non-public Facebook wall posts are protected under the Federal Stored Communications Act (the "SCA").
- Passed in 1986, the SCA provides protection to electronic communications that are configured to be private. The statutory language was drafted to address the potential privacy issues that could occur in the technology that existed in 1986, and the courts are tasked with adapting the language to modern technology.
- The statutory language in the SCA protects: "(1) electronic communications, (2) that were transmitted via an electronic communication service, (3) that are in electronic storage, and (4) that are not public."
- Although Facebook wall posts are covered under the SCA, the statute provides two exceptions: the SCA "does not apply with respect to conduct authorized (1) by the person or entity providing a wire or electronic communications service; [or] (2) by a user of that service with respect to a communication intended for that user."

FEDERAL STORED COMMUNICATIONS ACT

- *Ehling v. Monmouth-Ocean Hospital Service Corp.*, No. 2:11-CV-3305 (WMJ) (D.N.J. Aug. 20, 2013). The plaintiff was a registered nurse and paramedic at Monmouth-Ocean Hospital Service Corp. ("MONOC"). She maintained a personal Facebook profile and was "Facebook friends" with many of her coworkers but none of the MONOC managers. She adjusted her privacy preferences so only her "Facebook friends" could view the messages she posted onto her Facebook wall. Unbeknownst to the plaintiff, a coworker who was also a "Facebook friend" took screenshots of the plaintiff's wall posts and sent them to a MONOC manager. When the manager learned of a wall post in which the plaintiff criticized Washington, D.C. paramedics in their response to a museum shooting, MONOC temporarily suspended the plaintiff with pay and delivered a memo warning her that the wall post reflected a "deliberate disregard for patient safety." The plaintiff subsequently filed suit alleging violations of the SCA, among other claims.

- Although MONOC management never solicited or had direct access to the plaintiff's wall posts in any way, the District Court ruled that the wall posts were covered under the SCA. Addressing each criterion in turn, the District Court ruled that Facebook wall posts configured to be private are protected under the SCA. First, wall posts are electronic communications because Facebook users transmit data to Facebook servers when making a wall post. Second, the data from the wall post is transmitted via an electronic communication service because Facebook provides a service where users can send or receive electronic communications. Third, wall posts are in electronic storage because Facebook saves the information on a server immediately after the posting, and older posts are archived on separate pages that are still accessible to the user. Fourth, wall posts that are configured to be inaccessible to the general public are, by definition, not public.

- Very few courts have addressed the specific issue in this case, so it has been unclear whether Facebook posts are protected under the SCA. With the amount of information the modern person places onto social media, employers may find it convenient to use such information to make employment-related decisions. The federal court here, however, has made clear that non-public Facebook wall posts are indeed protected by the SCA, and employers may be held liable if they access such information without authorization. It is unclear whether the overall damages scheme has been altered considering the employer prevailed on the SCA claim, but the statute provides for a recovery floor of $1,000 consisting of the plaintiff's actual damages and the violator's profit, as well as costs and fees. Punitive damages may also be assessed for a willful or intentional violation. Although the company prevailed here because of the facts, employers should consider the SCA and other privacy issues when managing employees' social media use.

SOCIAL MEDIA AND THE CRIMINAL CASE: PEOPLE V. HARRIS

- Two decisions revolve around a criminal defendants use of twitter
- *People v Harris*, 36 Misc 3d 613 [Crim Ct, NY County April 2012]).
- *People v Harris*, 2012 NY Slip Op 22175 [36 Misc 3d 868 Criminal Ct. June 30, 2012]

SOCIAL MEDIA AND THE CRIMINAL CASE

- After On April 20, 2012, the court held that the defendant had no proprietary interest in the user information on his Twitter account, and he lacked standing to quash the subpoena) (i.e. bank accounts).
- Defendant had no privacy interest as well.
- The court's decision was partially based on Twitter's then terms of service agreement. After the April 20, 2012 decision, Twitter changed its terms and policy effective May 17, 2012. The newly added portion states: "You Retain Your Right To Any Content You Submit, Post Or Display On Or Through The Service

PEOPLE V. HARRIS

- *People v. Harris*, 2012 NY Slip Op 22175 [36 Misc 3d 868 Criminal Ct. June 30, 2012]
- The court then ordered Twitter to provide certain information to the court for in camera review to safeguard the privacy rights of Mr. Harris. Twitter sought to quash a subpoena issued by the New York County District Attorney‘s Office
- The Court noted that this was a case of first impression, distinctive because it is a criminal case rather than a civil case, and the movant is the corporate entity (Twitter) and not an individual (Harris). It also dealt with tweets that were publicly posted rather than an email or text that would be directed to a single person or a select few.

PEOPLE V. HARRIS

- Twitter argued that the court's decision to deny the defendant standing places an undue burden on Twitter. It forces Twitter to choose between either providing user communications and account information in response to all subpoenas or attempting to vindicate its users' rights by moving to quash these subpoenas itself. However, that burden is placed on every third-party respondent to a subpoena and cannot be used to create standing for a defendant where none exists.

- From the Court's perspective , publication to third parties was the issue. "Tweets are not emails sent to a single party. At best, the defense may argue that this is more akin to an email that is sent to a party and carbon copied to hundreds of others." The Court found that there can be no reasonable expectation of privacy in a tweet sent around the world. And that the court order was not unreasonably burdensome to Twitter, as it does not take much to search and provide the data to the court. "So long as the third party is in possession of the materials, the court may issue an order for the materials from the third party when the materials are relevant and evidentiary . '

  - Consider the following: a man walks to his window, opens the window, and screams down to a young lady, "I'm sorry I hit you, please come back upstairs." At trial, the People call a person who was walking across the street at the time this occurred. The prosecutor asks, "What did the defendant yell?" Clearly the answer is relevant and the witness could be compelled to testify. Well today, the street is an online, information superhighway, and the witnesses can be the third-party providers like Twitter, Facebook, Instragram, Pinterest, or the next hot social media application.

PEOPLE V. HARRIS

- The Court Order further found that the defendant had purposely broadcasted to the entire world into a server 3,000 miles away and therefore, the defendant's account is protected by the Fourth Amendment only if "the government violate[d] a subjective expectation of privacy that society recognizes as reasonable

  - If you post a tweet, just like if you scream it out the window, there is no reasonable expectation of privacy. There is no proprietary interest in your tweets, which you have now gifted to the world. This is not the same as a private email, a private direct message, a private chat, or any of the other readily available ways to have a private conversation via the Internet that now exist. Those private dialogues would require a warrant based on probable cause in order to access the relevant information.

- There is no reasonable expectation of privacy for tweets that the user has made public. It is the act of tweeting or disseminating communications to the public that controls. Even when a user deletes his or her tweets there are search engines available such as "Untweetable," "Tweleted" and "Politwoops" that hold users accountable for everything they had publicly tweeted and later deleted. Therefore, the defendant's Fourth Amendment rights were not violated because there was no physical intrusion of the defendant's tweets and the defendant has no reasonable expectation of privacy in the information he intentionally broadcasted to the world.

PEOPLE V. HARRIS

- As for the Stored Communications Act, the court found that defendant's anticipated trial defense is that the police either led or escorted him onto the non-pedestrian part of the Brooklyn Bridge, a defense allegedly contradicted by his publicly posted tweets around the time of the incident. The People were seeking two types of information, non-content information such as subscriber information, email addresses, etc. and content information such as tweets. The SCA protects only private communications and allows disclosure of electronic communication when it is not overbroad.

- In general, court orders have no limitations on the types of information to be disclosed (18 USC § 2703 [d]). The SCA mandates different standards that the government must satisfy to compel a provider to disclose various types of information (18 USC § 2703). To compel a provider of ECS to disclose the contents of communication in its possession that are in temporary "electronic storage" for 180 days or less, the government must obtain a search warrant (18 USC § 2703 [a]). A court order must be issued to compel a provider of ECS to disclose contents in electronic storage for greater than 180 days or to compel a provider of RCS to disclose its contents (18 USC § 2703 [a], [b], [d]). The law governing compelled disclosure also covers the above-mentioned non-content records. The rules are the same for providers of ECS and RCS and the government can obtain a section 2703 (d) order to compel such non-content information (18 USC § 2703 [c] [1] [B]).

- Thus the court ruled that the non-content records such as subscriber information, logs maintained by the network server, etc. and the September 15,2011 to December 30, 2011 tweets are covered by the court order. However, the government must obtain a search warrant for the December 31, 2011 tweets.

PEOPLE v. WELTE, 31 Misc.3d 867 , 920 N.Y.S.2d 627 (Justice Court of Town of Webster, Monroe County (2011)

- **Issues Presented**
- Does communication to a person's acquaintances listed as friends on a Facebook account violate a no contact order of protection?
- Does communication to a person's acquaintances listed as friends on a Facebook account constitute stalking in the fourth degree?

PEOPLE v. WELTE, 31 Misc.3d 867 , 920 N.Y.S.2d 627 (Justice Court of Town of Webster, Monroe County (2011)

- In the instant case the defendant's action in contacting the complainant's friends and family via her "Friends List" would not in the normal course of events violate any provision of law.
- In addition, the defendant was not directed to stay away from the friends and family of the complainant. Lastly, the accusatory instruments do not allege that the defendant was intentionally attempting to contact the complainant through her Friends List, only that the defendant was not to contact her through a third person.
- As a result, the information herein neither sets out "facts of an evidentiary character supporting or tending to support the charges" as required by CPL 100.15 (3), nor does the information allege "every element of the offense charged and the defendant's commission thereof" as required by CPL 100.40 (1).

Facebook and the Jury

- PEOPLE v. WILSON, 93 A.D.3d 483 , 939 N.Y.S.2d 463 (1st Dept (2012)
- The court denied defendant's CPL 330.30 (2) motion to set aside the verdict on the ground of juror misconduct on the grounds that a juror had made Facebook posting about the trial during the trial.
- The court found no basis for disturbing its credibility determinations. The juror made Facebook postings that merely advised her friends that she was on a jury, but did not discuss the case in any way. Some of her friends made replies relating to trials in general that defendant characterizes as "inflammatory."
- However, the juror testified unequivocally that she was not affected by these comments, that she did not discuss the case with anyone during the trial, and that she had decided the case impartially, based only on the evidence.

Facebook and the Jury

- People v. Rios, 26 Misc.3d 1225(a0, 907 N.Y. S. 2d 440 (Sup. Ct. Bronx 2010).
- A jury found defendants, an owner of an apartment building and its manager, guilty of Criminally Negligent Homicide and Reckless Endangerment in the Second Degree, arising out of the deaths of two New York City firefighters.
- During the adjournment period, the People disclosed to the court and the parties information regarding a juror's communications with a firefighter witness on a social networking web site.
- The court held that the defendants failed to elicit any testimony to establish what exactly the juror's "feelings" were or how any "feelings" implicit in her friend request affected the jury's deliberations in any way. Accordingly, defendants failed to meet their burden of establishing that the juror's misconduct prejudiced a substantial right of the defendants and denied to set aside the verdict based on juror misconduct are denied.

Facebook Fopars

- 

SOCIAL MEDIA AND DISCOVERY

- *Reid v. Ingerman Smith, LLP* (E.D.N.Y Dec. 27, 2012), Magistrate Judge Marilyn D. Go granted (and denied in part) a motion to compel discovery of plaintiff Reid's social media usage. The case itself revolves around a sexual harassment claim brought by Reid against Ingerman Smith for an incident while Reid was employed as a legal secretary.

  Judge Go agreed with the defendants that Reid's Facebook postings and comments on photographs placed on Facebook were relevant to whether Reid had actually experienced the emotional distress she claimed resulted from the sexual harassment. The court reviewed how other jurisdictions had dealt with similar questions, after observing that: "[a]although the law regarding the scope of discovery of electronically stored information ("ESI") is still unsettled, there is no dispute that social media information may be a source of relevant information that is discoverable." The ultimate issue, then, as summarized by the court:

- The defendants argued that since postings and photographs from the public portions of plaintiff's Facebook account contain information that contradict plaintiff's claims of mental anguish resulting from the alleged sexual harassment by defendant Sadowski and termination of her employment, the non-public portions may also provide relevant information. Plaintiff responded that she should not be subject to broad discovery of the entirety of her social media account and be required to disclose private information.

- Considerations for any court (1) facilitate discovery of information that is no doubt relevant to the claims in the case, but more importantly, (2) attempting to prevent further emotional damage to the plaintiff, whose privacy was already violated once by the sexual harassment, by limiting the reach of the prying inquiry requested by the defendant

SOCIAL MEDIA AND DISCOVERY

- *Pereira v City of New York* 2013 NY Slip Op 51091(U) Decided on June 19, 2013 Supreme Court, Queens County.

- Defendant moved for an order, inter alia, precluding plaintiff from testifying or offering any medical evidence at trial upon his failure to provide discovery in this personal injury action.

- The parties entered into a stipulation at the Compliance Conference of this action on December 12, 2012, so-ordered by the Hon. Martin E. Ritholtz, which directed plaintiff to "provide authorizations for Facebook Profile/MySpace Profile" within twenty days. It further provided that defendants had reserved the right to in-camera inspection of the complete Facebook and MySpace accounts, upon a showing of relevance to injuries alleged. Plaintiff failed to timely provide a response. Thereafter, defendants brought the within motion to preclude plaintiff from testifying or offering any medical evidence at trial upon his failure to provide discovery.
- Defendants have demonstrated that the photographs contained in plaintiff's Facebook profile and hockey blog were probative of the issue of the extent of plaintiff's alleged injuries. It is therefore reasonable to believe that other portions of his Facebook account may contain further evidence relevant to the issue of plaintiff's injuries. Accordingly, with respect to plaintiff's Facebook profile, the defendants have made "a showing that at least some of the discovery sought will result in the disclosure of relevant evidence or is reasonably calculated to lead to the discovery of information" bearing on his claim. See, Richards v. Hertz Corp., 100 AD3d 728 (2nd Dept. 2012).
- The Court directed Plaintiff to provide this court for in camera inspection, all photographs depicting sporting activities posted on the demanded media sites. While these media accounts may also contain other items such as status reports, e-mails, and videos that are relevant to the extent of plaintiff's alleged injuries, due to the likely presence of material of a private nature that is not relevant to this action, this court shall conduct an in camera inspection of copies of all status reports, e-mails, photographs, and videos posted on plaintiff's media sites since the date of the subject accident, to determine which of those materials, if any, are relevant to his alleged injuries.

SOCIAL MEDIA AND DISCOVERY

- The court summed up its thoughts as follows:

While plaintiff is correct that disclosure of her personal social media account may raise privacy concerns, such a consideration is more "germane to the question of whether requested discovery is burdensome or oppressive and whether it has been sought for a proper purpose" rather than to affording a "basis for shielding those communications from discovery." E.E.O.C. v. Simply Storage Mgmt., 270 F.R.D. 430, 434 (S.D. Ind. 2010). Even had plaintiff used privacy settings that allowed only her "friends" on Facebook to see postings, she "had no justifiable expectation that h[er] 'friends' would keep h[er] profile private . . ." U.S. v. Meregildo, 2012 U.S. Dist. LEXIS 115085, 2012 WL 3264501, at *2 (S.D.N.Y. 2012). In fact, "the wider h[er] circle of 'friends,' the more likely [her] posts would be viewed by someone [s]he never expected to see them." Id. *Thus, as the Second Circuit has recognized, legitimate expectations of privacy may be lower in e-mails or other Internet transmissions.* U.S. v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (contrasting privacy expectation of e-mail with greater expectation of privacy of materials located on a person's computer). (emphasis added)While many courts have stated that Internet communications are less protected, I'm not convinced that you can fully analogize a Facebook posting to an email. Here's why: An email has no built in protection to prevent forwarding to third parties; Facebook does - you personally limit who can see what on your page, and that effort in and of itself shows a subjective intent to retain an expectation of privacy in those posts. It is not a difference in kind, and I would never argue it was, but the continual need to analogize differing internet communications to email to appeal to more settled court precedent is troublesome.

The court eventually held that statements regarding plaintiff's social activities may be relevant to plaintiff's claims of emotional distress and loss of enjoyment of life. The postings may also provide information regarding potential witnesses with knowledge. ***Thus, plaintiff must disclose social media communications and photographs "that reveal, refer, or relate to any emotion, feeling, or mental state . . . [and] that reveal, refer, or relate to events that could reasonably expected to produce a significant emotion, feeling or mental state."*** Simply Storage, 270 F.R.D at 435-36; see also In re Air Crash, 2011 WL 6270189, at *6 (W.D.N.Y. 2011) . Likewise, photographs uploaded by plaintiff, a***s well as photographs uploaded by third parties depicting plaintiff are discoverable***, while other photographs that have a more tenuous connection with the party are less likely to be relevant. Clearly, "pictures of the claimant . . . will generally be discoverable because the context of the picture and the claimant's appearance may reveal the claimant's emotional or mental status" while "a picture posted on a third party's profile in which a claimant is merely 'tagged' is less likely to be relevant." Simply Storage, 270 F.R.D. at 436.

SOCIAL MEDIA AND DISCOVERY

- *Romano v. Steelcase Inc.*, 30 Misc.3d 426, 907 N.Y.S.2d 650, 2010 N.Y. Slip Op. 20388 (N.Y.Sup. Sep 21, 2010)
- In this case where plaintiff's alleged loss of enjoyment of life was at issue, the Supreme Court, Suffolk County, Justice Jeffrey Arlen Spinner, held that:
- (1) private information sought from plaintiff's social networking website accounts was material and necessary for defendant's defense;
- (2) plaintiff did not have a reasonable expectation of privacy in information published on social networking websites; and
- (3) defendant's need for access to plaintiff's private information on social networking websites outweighed any privacy concerns voiced by plaintiff.
- Because of lack of New York law, the court relied on *Ledbetter v. Wal–Mart Stores Inc.*, (06–cv–01958–WYD–MJW, 2009 WL 1067018 [D. Colo. April 21, 2009]), and *Leduc v. Roman*, 2009 CarswellOnt 843 (February 20, 2009), a matter pending in the Superior Court of Justice, Ontario, Canada. The Court observed that New York courts have yet to address whether there exists a right to privacy regarding what one posts on their on-line social networking pages such as Facebook and MySpace. However, whether one has a reasonable expectation of privacy in internet postings or e-mails that have reached their recipients has been addressed by the Second Circuit, which has held that individuals may not enjoy such an expectation of privacy (see: U.S. v. Lifshitz, 369 F.3d 173 [2d. Cir.2004]

SOCIAL MEDIA AND DISCOVERY

- But see in *Giacchetto v. Patchogue-Medford Union Free School Dist.,* 2013 WL 2897054 (E.D.N.Y. May 06, 2013) United States Magistrate Judge A. KATHLEEN TOMLINSON questioned the holding in Romano stating:

  - Some courts have held that the private section of a Facebook account is only discoverable if the party seeking the information can make a threshold evidentiary showing that the plaintiff's public Facebook profile contains information that undermines the plaintiff's claims (i.e. Romano).
  - This approach can lead to results that are both too broad and too narrow. On the one hand, a plaintiff should not be required to turn over the private section of his or her Facebook profile (which may or may not contain relevant information) merely because the public section undermines the plaintiff's claims. On the other hand, a plaintiff should be required to review the private section and produce any relevant information, regardless of what is reflected in the public section. The Federal Rules of Civil Procedure do not require a party to prove the existence of relevant material before requesting it. Furthermore, this approach improperly shields from discovery the information of Facebook users who do not share any information publicly. For all of the foregoing reasons, the Court will conduct a traditional relevance analysis.

SOCIAL MEDIA AND DISCOVERY

- M.J. Tomlinson directed that Plaintiffs postings be reviewed for relevance by **Plaintiff's counsel and that Plaintiff's counsel**— not Plaintiff—make a determination regarding the relevance of the postings, keeping in mind the broad scope of discovery contemplated under Rule 26. For support of this approach, the court cited

- *Howell v. Buckeye Ranch, Inc.,* 2012 WL 5265170, 116 (S.D.Ohio Oct 01, 2012) (ordering plaintiff's counsel to access plaintiff's social media accounts and produce responsive information as opposed to having plaintiff provide defendant with her usernames and passwords);

- *Anthony v. Atlantic Gr., Inc*., No. 09–CV–2942, 2012 WL 4009490, at *2 (D.S.C. Sept. 12, 2012) (directing plaintiff to access and produce social networking postings directly as opposed to having defendant seek the information from the service providers);

- *In re White Tail Oilfield Servs., L.L.C*., No. 11–CV–0009, 2012 WL 4857777, at *3 (E.D.La. Oct. 11, 2012) (directing party to download and produce Facebook information);

- *In re Air Crash Near Clarence Ctr., New York,* No. 09–md–2085, 2011 WL 6370189, at *6 (W.D.N.Y. Dec. 20, 2011) (denying request for authorizations subject to renewal if plaintiff's production was insufficient).

SOCIAL MEDIA AND DISCOVERY

- *Loporcaro v. City of New York*, 35 Misc.3d 1209(A), 950 N.Y.S.2d 723, 2012 N.Y. Slip Op. 50617(U) (N.Y.Sup. Apr 09, 2012)

- It is the opinion of this Court, that the moving defendant has sufficiently shown that information contained within plaintiff's Facebook account may contain information that is relevant to the claims made with regard to the effects of his injuries as alleged in their bill of particulars. These include plaintiff's claim to have been incapacitated and confined to bed or home during the first two months following the accident, as well as its permanent effects on his daily life.
- When a person creates a Facebook account, he or she may be found to have consented to the possibility that personal information might be shared with others, notwithstanding his or her privacy settings, as there is no guarantee that the pictures and information posted thereon, whether personal or not, will not be further broadcast and made available to other members of the public.
- Clearly, our present discovery statutes do not allow that the contents of such accounts should be treated differently from the rules applied to any other discovery material, and it is impossible to determine at this juncture whether any such disclosures may prove relevant to rebut plaintiffs' claims regarding, e.g., the permanent effects of the subject injury. Since it appears that plaintiff has voluntarily posted at least some information about himself on Facebook which may contradict the claims made by him in the present action, he cannot claim that these postings are now somehow privileged or immune from discovery.

SOCIAL MEDIA AND DISCOVERY

- Do not conduct a “Fishing expedition”

- *McCann v. Harleysville Ins. Co. of New York*, 78 A.D.3d 1524, 910 N.Y.S.2d 614, 2010 N.Y. Slip Op. 08181 (4th Dep’t Nov. 12, 2010).

- Plaintiff commenced an action seeking damages for injuries she sustained when the vehicle she was operating collided with a vehicle driven by defendant's insured. Defendant appealed from an order denying its motion to compel disclosure of photographs and seeking “an authorization for plaintiff's Facebook account.” According to defendant, the information sought was relevant with respect to the issue whether plaintiff sustained a serious injury in the accident. The Court concluded that Supreme Court properly denied defendant's motion “as overly broad,” without prejudice “to service of new, proper discovery demands”

- Although defendant specified the type of evidence sought, it failed to establish a factual predicate with respect to the relevancy of the evidence Indeed, defendant essentially sought permission to conduct “a fishing expedition” into plaintiff's Facebook account based on the mere hope of finding relevant evidence . However, the 4th Department found that the lower court abused its discretion in prohibiting defendant from seeking disclosure of plaintiff's Facebook account at a future date.

SOCIAL MEDIA AND DISCOVERY

- Do not conduct a “Fishing expedition”

- *Kregg v. Maldonado*, 98 A.D.3d 1289, 951 N.Y.S.2d 301, 2012 N.Y. Slip Op. 06454 (N.Y.A.D. 4th Dep’t Sep. 28, 2012)
- Plaintiff appealed from an order insofar as it granted that part of the motion of defendants Suzuki Motor Corporation of Japan and American Suzuki Motor Corporation to compel the disclosure of all social media account records concerning plaintiff's son , who was involved in a motor vehicle accident while driving a motorcycle manufactured and distributed by the Suzuki defendants

- In reversing the lower court , it was held that there is no contention that the information in the social media accounts contradicts plaintiff's claims for the diminution of the injured party's enjoyment of life (*cf.* *Romano v. Steelcase, Inc.,* 30 Misc.3d 426, 427, 907 N.Y.S.2d 650). As in *McCann,* the proper means by which to obtain disclosure of any relevant information contained in the social media accounts is a narrowly-tailored discovery request seeking only that social-media-based information that relates to the claimed injuries arising from the accident. Thus, it denied the Suzuki defendants' motion to compel “the disclosure of the entire contents of the injured party's social media accounts, without prejudice to the service of a more narrowly-tailored disclosure request.”

SOCIAL MEDIA AND DISCOVERY

- *Winchell v. Lopiccolo*, 38 Misc.3d 458, 954 N.Y.S.2d 421, 2012 N.Y. Slip Op. 22337 (N.Y.Sup. Oct 19, 2012)

- Defendants request authorization to access Plaintiff's Facebook page for the purpose of discovering what it reveals about Plaintiff's "ability to portray cognitive function.". Defendants further clarified their request as follows:
- "the layout of her Facebook page would demonstrate cognitive function inasmuch as the layout of a Facebook page calls for creativity of some sort as well as thought in providing captions for photographs, narrative posts written by the plaintiff as well as her ability to write and comment. Writings on the page would be direct and circumstantial evidence of her claims. Moreover, lucid and logical writing or a lack thereof, would be useful in the defense and/or assessment of this case."
- "The Court finds that there is a dearth of case law in this emerging area regarding discovery of electronic and digital information. In fact, at least one court, in its quest for guidance, went so far as to consult Canadian law. See Romano . Discovery in this area is nonetheless governed by the same legal principles that guide more traditional forms of discovery and, as one court put it, "digital 'fishing expeditions' are no less objectionable than their analog antecedents." Caraballo v. City of New York, 2011 N.Y. Slip Op. 30605(U), 2011 WL 972547 [Sup. Ct. Richmond County 2011].
- The party demanding access to social networking accounts must show that the method of discovery will lead to "the disclosure of relevant evidence or is reasonably calculated to lead to the discovery of information that bears on the claims.

SOCIAL MEDIA AND DISCOVERY

- *Tapp v. New York State Urban Development Corp*., 102 A.D.3d 620, 958 N.Y.S.2d 392, 2013 N.Y. Slip Op. 00547 (1st Dep't Jan. 31, 2013)
- The motion court correctly determined that plaintiff's mere possession and utilization of a Facebook account is an insufficient basis to compel plaintiff to provide access to the account or to have the court conduct an in camera inspection of the account's usage. To warrant discovery, defendants must establish a factual predicate for their request by identifying relevant information in plaintiff's Facebook account—that is, information that "contradicts or conflicts with plaintiff's alleged restrictions, disabilities, and losses, and other claims. Defendants failed to identify relevant information.

- Defendants' argument that plaintiff's Facebook postings "may reveal daily activities that contradict or conflict with" plaintiff's claim of disability amounts to nothing more than a request for permission to conduct a "fishing expedition"

SOCIAL MEDIA AND DISCOVERY:
IN CAMARA INSPECTION

- *Richards v. Hertz Corp*., 100 A.D.3d 728, 953 N.Y.S.2d 654, 2012 N.Y. Slip Op. 07650 (2d Dep't Nov. 14, 2012) –
- The defendants demonstrated that one of the plaintiff's Facebook profile s sought contained a photograph that was probative of the issue of the extent of her alleged injuries, and it is reasonable to believe that other portions of her Facebook profile may contain further evidence relevant to that issue. Thus, they made a showing that at least some of the discovery sought will result in the disclosure of relevant evidence or is reasonably calculated to lead to the discovery of information bearing on her).
- However, while the Supreme Court directed the injured plaintiffs to provide copies of photographs depicting them participating in sporting activities, the Facebook profile may also contain other items such as status reports, e-mails, and videos that are relevant to the extent of her alleged injuries.
- Due to the likely presence in plaintiff's Facebook profile of material of a private nature that is not relevant to this action, the Supreme Court should conduct an in camera inspection of all status reports, e-mails, photographs, and videos posted on theFacebook profile since the date of the subject accident to determine which of those materials, if any, are relevant to her alleged injuries.

SOCIAL MEDIA AND DISCOVERY

- *Nieves v. 30 Ellwood Realty LLC*, 39 Misc.3d 63, 966 N.Y.S.2d 808, 2013 N.Y. Slip Op. 23128 (N.Y.Sup.App.Term Apr 11, 2013)
- Defendant demonstrated that plaintiff's Facebook profile contained photographs that were probative of the issue of the extent of her alleged injuries, and it is reasonable to believe that other portions of her Facebook records may contain further evidence relevant to that
- In these circumstances, and since "it is possible that not all Facebook communications are related to the events that gave rise to plaintiff's cause of action" the appropriate course is to remand the matter for an in camera inspection of plaintiff's Facebook records, to determine which of those records, if any, are relevant to plaintiff's alleged injuries. To the extent that a thorough in camera inspection may prove unduly burdensome, the trial court retains broad discretion to set reasonable terms and conditions thereon including the right to direct plaintiff to conduct an initial review of her own Facebook account, and limit the in camera inspection to items whose discoverability is contested by plaintiff.

SOCIAL MEDIA AND EVIDENCE

- The Primary Issues:
- (1) Authentication
- (2) Admissibility

SOCIAL MEDIA AND EVIDENCE

To authenticate social media based evidence. One must go back to the basic and understand what is "authentication"

To "authenticate' evidence the party must show that the item is what it purports to be. Judge Friendly put the matter as follows: "Authentication is perhaps the purest example of a rule respecting relevance: evidence admitted as something can have no probative value unless that is what it really is.", The process of authentication and identification, often called laying a foundation

In New York, the applicable standard of proof on issues of authentication, as well as the allocation of responsibility between judge and jury, is less clear than in federal practice. In People v. McGee, the Court of Appeals made the following statement: "In determining whether a proper foundation has been laid for the introduction of real evidence, the accuracy of the object itself is the focus of inquiry, which must be demonstrated by clear and convincing evidence.

Under the federal Rules of Evidence Rule 901(a) of the Federal Rules of Evidence provides:

(a) In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.

But how, exactly, does a lawyer make the jump from the computer screen to the courtroom?

Unless uncontroverted and cooperative witness testimony is available, the proponent must rely on other means to establish a proper foundation. A party can authenticate electronically stored information ("ESI") per Rule 901(b)(4) with circumstantial evidence that reflects the "contents, substance, internal patterns, or other distinctive characteristics" of the evidence. Many courts have applied Rule 901(b)(4) by ruling that metadata and file level hash values associated with ESI can be sufficient circumstantial evidence to establish its authenticity.

As the paper further explains, metadata and file level hash values are not easy to preserve when collecting social media--based evidence. Preservation and authentication of ESI is a highly technical and specialized field.

One option to help ensure eventual authentication of social media--based evidence is, of course, to hire a professional engaged in the business of preserving this data. Although it may be expensive to hire an e-discovery expert, the initial expense is likely to be outweighed by the future benefit. To keep the cost of litigation manageable, it may make sense to have an investigator or paralegal perform the initial research and then follow up with a professional, if appropriate

SOCIAL MEDIA AND EVIDENCE

Griffin v. State, 419 Md. 343, 19 A.3d 415 (Md. Apr. 28, 2011)

- Griffin was charged in numerous counts with the shooting death, on April 24, 2005, of Darvell Guest at Ferrari's Bar in Perryville, in Cecil County Maryland. During his trial, the State sought to introduce Griffin's girlfriend's, Jessica Barber's, MySpace profile to demonstrate that, prior to trial, Ms. Barber had allegedly threatened another witness called by the State. The printed pages contained a MySpace profile in the name of "Sistasouljah," describing a 23 year-old female from Port Deposit, listing her birthday as "10/02/1983" and containing a photograph of an embracing couple. The printed pages also contained the following blurb:

- FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!

SOCIAL MEDIA AND EVIDENCE

Griffin v. State, 419 Md. 343, 19 A.3d 415 (Md. Apr. 28, 2011)

- After Griffin's conviction, Griffin argued that the State did not appropriately, for evidentiary purposes, authenticate pages allegedly printed from the victims MySpace profile, because the State failed to offer any extrinsic evidence describing MySpace, as well as indicating how the Police obtained the pages in question and adequately linking both the profile and the "snitches get stitches" posting to Ms. Barber. The State countered that the photograph, personal information, and references to freeing "Boozy" were sufficient to enable the finder of fact to believe that the pages printed from MySpace were indeed Ms. Barber's.

SOCIAL MEDIA AND EVIDENCE

Griffin v. State, 419 Md. 343, 19 A.3d 415 (Md. Apr 28, 2011)

- The Court was critical of the Court of Special Appeals view, who gave short shrift to the concern that “someone other than the alleged author may have accessed the account and posted the message in question.”
- “ While the intermediate appellate court determined that the pages allegedly printed from Ms. Barber's MySpace profile contained sufficient indicia of reliability, because the printout “featured a photograph of Ms. Barber and [Petitioner] in an embrace,” and also contained the “user's birth date and identified her boyfriend as ‘Boozy,’ ” the court failed to acknowledge the possibility or likelihood that another user could have created the profile in issue or authored the “snitches get stitches” posting.”

SOCIAL MEDIA AND EVIDENCE

Griffin v. State, 419 Md. 343, 19 A.3d 415 (Md. Apr 28, 2011)

- The picture of Ms. Barber, coupled with her birth date and location, were not sufficient "distinctive characteristics" on a MySpace profile to authenticate its printout, given the prospect that someone other than Ms. Barber could have not only created the site, but also posted the "snitches get stitches" comment.
- The potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user leads to our conclusion that a printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site in order to reflect that Ms. Barber was its creator and the author of the "snitches get stitches."

SOCIAL MEDIA AND EVIDENCE

How to get over the authentication hump?

Answer the Question: Could anyone but the individual who it is being offered against access the website where the picture/document was found?

See Rule 901. Authenticating or Identifying Evidence (b) Examples. The following are examples only — not a complete list — of evidence that satisfies the authentication requirement:

(4) Distinctive Characteristics and the Like. The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances.

SOCIAL MEDIA AND EVIDENCE

Foundational Questions:

- When did you establish the web page?
- Have you ever notified the website that your page had been hacked?
- Did you go through each piece of information on the site and establish its accuracy and personal connection to the witness?

SOCIAL MEDIA AND EVIDENCE

U.S. v. Gagliardi, 506 F.3d 140 (2nd Cir.(N.Y.) Oct 22, 2007)

Gagliardi's claimed that the e-mails and transcripts of instant-message chats offered by the government were not properly authenticated. He argued that because the documents were largely cut from his electronic communications and then pasted into word processing files, they were not originals and could have been subject to editing by the government. Gagliardi contended that the communications could even have been completely fabricated. Due to these "highly suspicious" circumstances, Gagliardi submitted that the government failed to establish authenticity and the trial court therefore erred in admitting the evidence.

The Court held that "the bar for authentication of evidence is not particularly high." United States v. Dhinsa, 243 F.3d 635, 658 (2d Cir.2001). "The requirement of authentication ... is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Fed.R.Evid. 901(a). Generally, a document is properly authenticated if a reasonable juror could find in favor of authenticity. United States v. Tin Yat Chin, 371 F.3d 31, 38 (2d Cir.2004). The proponent need not "rule out all possibilities inconsistent with authenticity, or to prove beyond any doubt that the evidence is what it purports to be." United States v. Pluta, 176 F.3d 43, 49 (2d Cir.1999) (internal quotation marks and citation omitted).

The Court added that "[w]e have stated that the standard for authentication is one of "reasonable likelihood," id. (internal quotation marks and citation omitted), and is "minimal," Tin Yat Chin, 371 F.3d at 38. The testimony of a witness with knowledge that a matter is what it is claimed to be is sufficient to satisfy this standard. See Fed.R.Evid. 901(b)(1). In this case, both the informant and Agent Berglas testified that the exhibits were in fact accurate records of Gagliardi's conversations with Lorie and Julie. Based on their testimony, a reasonable juror could have found that the exhibits did represent those conversations, notwithstanding that the e-mails and online chats were editable. The district court did not abuse its discretion in admitting the documents into evidence.

SOCIAL MEDIA AND EVIDENCE

- *Johnson v. Ingalls*, 95 A.D.3d 1398, 944 N.Y.S.2d 654, 279 Ed. Law Rep. 1108, 2012 N.Y. Slip Op. 03492 (N.Y.A.D. 3 Dept. May 03, 2012)
- The Court rejected plaintiff's contention that certain photographs obtained from her Facebook account were unduly prejudicial and improperly admitted into evidence.
- Plaintiff claimed that, as a result of her injury, she suffered severe anxiety, vertigo, constant migraines and pain for a period of about two years, that her anxiety prevented her from going out or socializing with friends, and that she required antidepressant medication.
- The photos admitted were taken over a 1 1/2-year period beginning shortly after the accident. They depicted plaintiff attending parties, socializing and vacationing with friends, dancing, drinking beer in an inverted position referred to in testimony as a "keg stand," and otherwise appearing to be active, socially engaged and happy. They further revealed that plaintiff consumed alcohol during this period, contrary to medical advice and her reports to her physicians. The discretion of trial courts in rendering evidentiary rulings is broad .The photographs had probative value with regard to plaintiff's claimed injuries, their evidentiary value was properly balanced against their potential for prejudice, and we find no abuse of discretion

SOCIAL MEDIA AND EVIDENCE

- Are statements made on Social media websites hearsay?
- *Lorraine v. Market American Ins. Co*., 241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446 (D.Md. May 04, 2007)
- The key to understanding the hearsay rule is to appreciate that it only applies to intentionally assertive verbal or non-verbal conduct, and its goal is to guard against the risks associated with testimonial evidence: perception, memory, sincerity and narration. Fed.R.Evid. 801 advisory committee's note ;Weinstein at § 801. 11[1] (“To be considered hearsay, a statement out of court must be offered in evidence to prove the truth of the matter it asserts. This part of the definition arises out of the factfinder's need to assess the credibility of the person who made a statement offered for its truth. When a witness testifies in court, the trier can assess the witness's perception, narration and memory to determine whether the testimony accurately represents the facts observed.”); Paul R. Rice, Electronic Evidence: Law and Practice, 262 (ABA Publishing 2005)(hereinafter “Rice”) (“Hearsay is an out-of-court statement offered in court to prove the truth of the matter asserted by the out-of-court declarant. It is offered into evidence through the testimony of a witness to that statement or through a written account by the declarant. The hearsay rule excludes such evidence because it possesses the testimonial dangers of perception, memory, sincerity, and ambiguity that cannot be tested through oath and cross-examination.”).

SOCIAL MEDIA AND EVIDENCE

- Are statements made on Social media websites hearsay?
- *Lorraine v. Markel American Ins. Co*., 241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446 (D.Md. May 04, 2007)
- The second question that must be answered in the hearsay analysis is closely tied to the first.
- A writing or spoken utterance cannot be a "statement" under the hearsay rule unless it is made by a "declarant," as required by Rule 801(b), which provides "[a] 'declarant' is a *person* who makes a statement." (emphasis added).
- When an electronically generated record is entirely the product of the functioning of a computerized system or process, such as the "report" generated when a fax is sent showing the number to which the fax was sent and the time it was received, there is no "person" involved in the creation of the record, and no "assertion" being made. For that reason, the record is not a statement and cannot be hearsay.

SOCIAL MEDIA AND EVIDENCE

- Are statements made on Social media websites hearsay?
- *Lorraine v. Markel American Ins. Co.,* 241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446 (D.Md. May 04, 2007)
- Cases involving electronic evidence often raise the issue of whether electronic writings constitute "statements" under Rule 801(a).
- Where the writings are non-assertive, or not made by a "person," courts have held that they do not constitute hearsay, as they are not "statements." United States v. Khorozian, 333 F.3d 498, 506 (3d Cir.2003) ("[N]either the header nor the text of the fax was hearsay. As to the header, '[u]nder FRE 801(a), a statement is something uttered by "a person," so nothing "said" by a machine ... is hearsay' ")
- Safavian, 435 F.Supp.2d at 44 (holding that portions of e-mail communications that make imperative statements instructing defendant what to do, or asking questions are nonassertive verbal conduct that does not fit within the definition of hearsay);
- Telewizja Polska USA, 2004 WL 2367740 (finding that images and text posted on website offered to show what the website looked like on a particular day were not "statements" and therefore fell outside the reach of the hearsay rule);
- Perfect 10, 213 F.Supp.2d at 1155 (finding that images and text taken from website of defendant not hearsay, "to the extent these images and text are being introduced to show the images and text found on the websites, they are not statements at all-and thus fall outside the ambit of the hearsay rule.");
- United States v. Rollins, rev'd on other grounds 2004 WL 26780, at *9 (A.F.Ct.Crim.App. Dec.24, 2003) ("Computer generated records are not hearsay: the role that the hearsay rule plays in limiting the fact finder's consideration to reliable evidence received from witnesses who are under oath and subject to cross-examination has no application to the computer generated record in this case. Instead, the admissibility of the computer tracing system record should be measured by the reliability of the system itself, relative to its proper functioning and accuracy.");

SOCIAL MEDIA AND EVIDENCE

- Are statements made on Social media websites hearsay?
- *Lorraine v. Markel American Ins. Co.,* 241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446 (D.Md. May 04, 2007)
- The requirement that the statement be offered to prove its substantive truth.
- The third question that must be answered in determining if evidence is hearsay is whether the statement is offered to prove its substantive truth, or for some other purpose.
- Rule 801(c) states: "Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." (emphasis added).
- Thus, even if the evidence is an assertion, made by a declarant, it still is not hearsay unless offered to prove the truth of what is asserted. The advisory committee's note to Rule 801(c) underscores this: "If the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted, and the statement is not hearsay. The effect is to exclude from hearsay the entire category of 'verbal acts' and 'verbal parts of an act,' in which the statement itself affects the legal rights of the parties or is a circumstance bearing on conduct affecting their rights." Fed.R.Evid. 801(c) advisory committee's note (citation omitted). See also Weinstein at § 801.11[1] (" 'If the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted.'
- Thus, if a declarant's statement is not offered for its truth, the declarant's credibility is not material, and the statement is not hearsay." (citation omitted)). Commentators have identified many instances in which assertive statements are not hearsay because they are not offered to prove the truth of the assertions: (1) statements offered to prove a claim that the statement was false or misleading, as in a fraud or misrepresentation case; (2) statements offered to "prove that because they were made, listeners had notice or knowledge of the information related in the statements," or to show the effect on the listener of the statement; (3) statements "offered to prove an association between two or more persons;" 4) statements offered as circumstantial evidence of the declarant's state of mind,FN45 or motive; (5) statements that have relevance simply because they were made, regardless of their literal truth or falsity-the so called "verbal acts or parts of acts," also referred to as "legally operative facts"; and (6) statements that are questions or imperative commands,such as "what time is it" or "close the door."

SOCIAL MEDIA AND EVIDENCE

- Are statements made on Social media websites hearsay?
- *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446 (D.Md. May 04, 2007)
- If they are hearsay –
- If, after applying the foregoing four-step analysis, it is determined that the electronic evidence constitutes a statement by a person that is offered for its substantive truth and is not excluded from the definition of hearsay by Rule 801(d)(1) or (2), then the evidence is hearsay, and is inadmissible unless it qualifies as one of many hearsay exceptions identified by Rule 803, 804 and 807.
- There twenty-three hearsay exceptions identified in Rule 803, five in Rule 804, and Rule 807, the so-called "catch-all" exception, allows exceptions to be tailor made. Upon closer examination, however, the task is less onerous because the number of hearsay exceptions can be categorized in helpful ways that make them more manageable, and in most instances a handful of hearsay exceptions repeatedly are used in connection with electronically generated or stored evidence. Familiarity with these rules will suffice in most instances to overcome hearsay objections routinely made to ESI.

SOCIAL MEDIA AND EVIDENCE

- Are statements made on Social media websites hearsay?
- *Lorraine v. Markel American Ins. Co.,* 241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446 (D.Md. May 04, 2007)
- When analyzing the admissibility of electronically generated evidence, courts also have held that statements contained within such evidence fall outside the hearsay definition if offered for a purpose other than their substantive truth. *Siddiqui,* 235 F.3d at 1323 (e-mail between defendant and co-worker not hearsay because not offered to prove truth of substantive content, but instead to show that a relationship existed between defendant and co-worker, and that it was customary for them to communicate by e-mail); *Safavian,* 435 F.Supp.2d at 44 (e-mail from lobbyist to defendant not hearsay because they were not offered to prove their truth, but to illustrate the nature of the lobbyist's work on behalf of clients to provide context for other admissible e-mail; and as evidence of the defendant's intent, motive and state of mind); *Telewizja Polska USA,* 2004 WL 2367740; *Perfect 10,* 213 F.Supp.2d at 1155 (exhibits of defendant's website on a particular date were not "statements" for purposes of hearsay rule because they were offered to show trademark and copyright infringement, therefore they were relevant for a purpose other than their literal truth); *State v. Braidic,* 119 Wash.App. 1075, 2004 WL 52412 at *1 (Jan. 13, 2004) (e-mail sent by defendant to victim not hearsay because they were not offered to prove the truth of the statements.).
- Finally, of particular relevance to this suit are the cases that have held that communications between the parties to a contract that define the terms of a contract, or prove its content, are not hearsay, as they are verbal acts or legally operative facts. *See, e.g., Preferred Properties Inc. v. Indian River Estates Inc.,* 276 F.3d 790, 799 n. 5 (6th Cir.2002) (verbal acts creating a contract are not hearsay); *Kepner-Tregoe, Inc. v. Leadership Software,* 12 F.3d 527, 540 (5th Cir.1994) (finding contract to be a signed writing of independent legal significance and therefore non-hearsay); *Mueller v. Abdnor,* 972 F.2d 931, 937 (8th Cir.1992) (holding contracts and letters from attorney relating to the formation thereof are non-hearsay); *United States v. Tann,* 425 F.Supp.2d 26, 29 (D.D.C.2006) (finding negotiable instruments to be legally operative documents that do not constitute hearsay); *Planmatics,* 137 F.Supp.2d at 621 (D.Md.2001) (holding testimony regarding instructions made to individuals is not hearsay because instructions were not statements of fact). *See also* WEINSTEIN at § 801.11[3].

SOCIAL MEDIA AND EVIDENCE

- Are the statements Admissions?
- Rule 801(d)(2) identifies five types of statements as “admissions by a party opponent,” and excludes them from the definition of hearsay. Specifically: 801(d)(2)(A) excludes the party's own statement, made in either an individual or representative capacity; 801(d)(2)(B) addresses a statement by another that a party has adopted or manifested a belief in its truth; 801(d)(2)(C) deals with a statement by a person authorized by a party to make a statement concerning a subject; 801(d)(2)(D) excludes a statement made by a party's agent or servant concerning a matter within the scope of the agency or employment, made during the existence of the agency or employment relationship; and 801(d)(2)(E) excludes the statement of a co-conspirator of a party made during the existence of the conspiracy and in furtherance of the conspiracy. To qualify as an admission, the party's out-of-court statement must be offered against that party, it cannot offer its own out of court statements as admissions. Weinstein at § 801.30[1] (“To be admissible under [Rule 801(d)(2)], the party's statements must be offered against that party. A party cannot use this provision to offer his or her own statements into evidence.”).
- As can be seen from reading Rule 801(d)(1) and (2), there are specific foundational facts that must be established before the statement or admission can be accepted into evidence. These determinations are made by the trial judge under Rule 104(a), and therefore the rules of evidence, except for privilege, are inapplicable. Fed.R.Evid. 104(a), 1101(d)(1); Fed.R.Evid. 104(a) advisory committee's note (“[W]hen a hearsay statement is offered as a declaration against interest, a decision must be made whether it possesses the required against-interest characteristics. These decisions too, are made by the judge.”)
- Given the near universal use of electronic means of communication, it is not surprising that statements contained in electronically made or stored evidence often have been found to qualify as admissions by a party opponent if offered against that party. Siddiqui, 235 F.3d at 1323 (ruling that e-mail authored by defendant was not hearsay because it was an admission under Rule 801(d)(2)(A)); Safavian, 435 F.Supp.2d at 43-44 (holding that e-mail sent by defendant himself was admissible as non-hearsay because it constituted an admission by the defendant, 801(d)(2)(A), and as an “adoptive admission” under Rule 801(d)(2)(B)); Telewizja Polska USA, 2004 WL 2367740 (N.D.Ill. Oct.15, 2004) (holding exhibits showing defendant's website as it appeared on a certain day were admissible as admissions against defendant); Perfect 10, 213 F.Supp.2d at 1155 (admitting e-mail sent by employees of defendant against the defendant as admissions under 801(d)(2)(D)).