5-6-2019

Discovery of Evidence with Social Media

John Wilkins
University of Mississippi

Discovery of Evidence with Social Media

John Wilkins

University of Mississippi

May 2019

A thesis submitted to the faculty of The University of Mississippi in partial fulfillment of the requirements of the Sally McDonnell Barksdale Honors College.

Approved by:

Adviser: Dr. Francis Boateng

Reader: Dr. Kimberly Kaiser

Reader: Dr. Teresa Carithers

Discovery of Evidence with Social Media

John Wilkins

University of Mississippi

May 2019

A thesis submitted to the faculty of The University of Mississippi in partial fulfillment of the requirements of the Sally McDonnell Barksdale Honors College.

Approved by:

Adviser: Dr. Francis Boateng

Reader: Dr. Kimberly Kaiser

Reader: Dr. Teresa Carithers

DEDICATION

For mom

Patricia Ruth Sagan Wilkins

April 7, 1956 - April 7, 2018

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

Advocacy is about the client, who is entitled to a thorough investigation of the facts. The formal fact gathering stage of litigation is discovery, which involves interrogatories, depositions, requests to produce, medical examinations, and requests for admission (Maerowitz & Mauet, 2013). Interrogatories and depositions give litigants a chance to posit questions regarding social media evidence. A social media post could be used to discredit and devalue prior witnesses' testimony. It could be particularly useful for attorneys and paralegals who find themselves lacking corroborating evidence to bolster their claims using online resources. Consider how websites such as Facebook, Instagram, and Twitter allow users to cultivate a reflection of their character online. The result is a database of digital-dossiers. Case law has shown that requests which are excessive in scope and which are not justified.

The fact is that the use of social media evidence has been a recent development, but it is here to stay. The American Academy of Matrimonial Lawyers - AAML(2010) found that 81% of top divorce attorneys reported a rise in the frequency of social media evidence in the courtroom. 66% reported that Facebook was the primary website being used. Social media evidence has emerged with courtroom application, and thus is a

valuable source of evidence. This law review will assert that social media has to be taken seriously as a source of evidence. It is widely used by two-thirds of Americans. It is an advancement in American life on par with the invention of the radio. We are communicating different. Thankfully, the law is compatible with this new form of interactive technology. This paper will act as a snapshot of social media evidence in the law as of 2019. By doing so, this paper will review Federal Rules of Evidence, Statutory law, and case law will be reviewed to lay the foundation of its applicability. In addition, the paper will also review the nature of social media as a communicative medium in order to show that it is a useful for attorneys. This involves reviewing statistics and scholarly articles which confirm the pervasive use and forms of content.

I. BACKGROUND

Social media has staying power in our lives. In fact, whether social media entails some qualities which are addictive has been explored and discussed in journal articles. Haynes wrote in *Science in the News* on the effects of social media usage, where he made comparisons between Las Vegas gambling and social media apps. “If we perceive a reward to be delivered at random, and if checking for the reward comes at little cost, we end up checking habitually (*e.g.* gambling addiction)” (Haynes, 2018). Social media companies seek the greatest amount of the public's attention to the social media website. It’s widely used as two-thirds of Americans report maintaining Facebook profiles (Smith & Anderson, 2018). A third of respondents use Instagram, SnapChat, and Twitter. In one form or another, it is likely that websites that host communities of people sharing their thoughts, private messages, and photos will persist as long as we have access to the internet. The brokerage firm Merrill Lynch identified Google, Instagram, FB Messenger, Facebook, and Yelp as having the greatest amount of stability among users (Lange, 2019). Users create scrollable pages of their personal lives which tend to reflect their opinions, life events, and social networks, which can then be utilized by attorneys. There is legal precedent in common law affecting the finer points of admitting direct messages,

text-posts, and photographic-posts, however the evidence is quite accessible in general. The Federal Rules of Evidence do not put much weight on the source of evidence so much as the relevance of the evidence. Social media seems to be highly accessible to attorneys who wish to vet all witnesses and parties involved in their litigation. This paper will highlight how lawyers can use social media to their benefit.

Discovery is the primary method used in gathering formal factual information for the purposes of litigation. This stage of the litigation process can prove highly consequential to the outcome of the case. The time and costs of actually going to trial are significant factors in the litigation process. Leveraging these factors in the discovery process can help induce a settlement agreement. Framing the exhausting process of litigation with the possibility of a favorable outcome is fundamental to achieving an out of court settlement. Additionally, the emergence of social media evidence created a source of evidence that was simply unavailable to past generations of lawyers. Attorneys who do not understand the incorporation of social media into the current discovery process could even potentially miss out on some of the positive impacts.

The parties in discovery obtain and disclose evidence prior to trial. At this stage, each side will become wholly aware of the strengths and weaknesses of their side of the case. Discovery can be eye-opening for the parties to an action and frequently encourages settlement agreements. Understanding the likely outcome of a case, coupled with the time and costs that go along with trial preparation, often results in the two parties reaching an agreement and foregoing trial altogether. The creation of social media websites has led to a virtual treasure trove of publicly accessible data. The emergence of social media

evidence has created an entire new realm of resources to build a stronger case, and hopefully invoke a settlement before going to trial. Given that discovery issues will most likely resolved before the conclusion of a trial; this stage of litigation can be a make or break moment for a client's case.

II. LITERATURE REVIEW

The inclusion of social media content into the existing rules of court is a developing area of law today. Social media websites give users the ability to interact with individuals, communities, organizations, and businesses in new and exciting ways. Content is predominantly user-produced and is in the form of text, photos, and video. The pervasive use of this communicative medium lends itself to the legal field as an invaluable evidentiary resource. The scope to which the information shared by users is admissible in the courts is unique to each case. However, what is shared on social media sites is generally discoverable by attorneys. The individual's reasonable expectation of privacy is often annulled if the request is limited to information relevant to the court case in question. Researchers have strong agreement about social media topics such as admissibility, value, and ethical considerations (Barnum, 2014; Brower et al., 2013; Gensler, 2012; Keefe, 2017; Medina, 2013, Moore, 2014; Trassati & Horevay, 2013).

Literature demonstrates that social media content is generally admissible in a court of law. The Federal Rules of Civil Procedure (FRCP) state that parties are allowed discovery of any matter so long as it is "reasonably calculated to lead to the discovery of

admissible evidence" (Fed. R. Civ. P. 34; c.f. Gensler, 2012, p. 14). In fact, social media is almost a nonissue because the scope of discovery has never considered the source of the information, i.e. medical records, financial records, police records. The scope of discovery is based on the information at issue. Trasatti and Horevay (2013) report that as of 2006, electronically stored information has been included among other admissible records (p. 262). Rule 26 of the FRCP gives parties the ability to obtain discovery of relevant and proportional to the needs of the case. In general, this makes social media discoverable given that the scope of discovery is not overly broad and is sufficiently relevant to the claim (Barnum, 2014; Keefe, 2017). According to the terms of use of both Facebook and Myspace, users cannot claim information they post to be privileged once posted. In situations where they share information, the user does not establish a reasonable expectation of privacy (Trasatti & Horevay, 2013). In 2013, Edward Snowden disclosed that social-media corporations the share information gleaned from their sites with the U.S. National Security Agency. The whistleblower described the collection of information to follow a "collect it all" doctrine (Lange, 2019). Moreover, courts have resolved that the very nature of social media websites as a forum for the sharing of information negates an individual's reasonable expectation of privacy (Moore, 2013). Social media is admissible in most cases where the evidence is sufficiently relevant, especially if it can be found on the publicly visible portion of the webpage.

A second pattern within the literature is that social media content is considered to be a valuable resource for evidence due to its pervasive use, candid content, and its courtroom applicability (Brower et al., 2013). The issues that surround the

implementation of social media in the courtroom have been published in the national legal press. The American Bar Association has stated that attorneys are obligated to warn clients of how their social media content may be used by third-parties against them. Equally important, the use of social media has surged in recent years with 71% of all Internet users found on Facebook, 22% on LinkedIn, 21% on Pinterest, 18% on Twitter, and 17% on Instagram (Trasatti & Horevay, 2013). Additionally, social networking use increases to 83% for internet users under age fifty according to Trasatti and Horevay (2013). The pervasive use of this technology has established it as a treasure-trove to the legal community. For example, Moore (2014) writes that status updates are broadly accessible to internet users and that the privacy settings that limit the initial audience of posts "encourages users to generate frank, informal, and often highly personal content" (p. 405). An audit of the opposing party's social media account may be revealing and have a substantial effect on the outcome of a case (Gensler, 2012). For instance, the plaintiff in *Zimmerman v. Weis Markets, Inc.* claimed injuries incurred from a forklift accident caused "serious, permanent health impairment and that scarring caused embarrassment so that he never wore shorts." Zimmerman filed the lawsuit against Weis Markets for injuries he suffered on the job. There existed a contracting relationship between Weis Markets and Zimmerman's employer. However, his Facebook contained photos of injuries from motorcycle accidents before and after the forklift accident. He made posts indicating that he enjoyed "bike stunts." Additionally, there were photos of the plaintiff in shorts (Brower, Longo, Lynn III, 2013).

Finally, there is a consensus among legal scholars for the ethical considerations that must be accounted for among witnesses, jurors, attorneys, and judges alike. Social media has the potential to bias all courtroom participants, which is why witnesses and jurors may not be connected with judges or attorneys on such websites. Lawyers may be tempted to discover whether a motion for discovery will be worthwhile for them. Most states have some form of rule barring attorneys from employing deception in order to "friend" an adverse party or witness, thereby gaining access to the private social media content (Keefe, 2017). It is ethical, however, for attorneys to view the publicly available portion of a social media page. These ethical considerations extend to jurors as well. For instance, Trasatti and Horevay (2013) describe the case of *State of West Virginia v. Dellinger,* Case No. 35273 (Va.Ct. App. June 3, 2010) in which a juror messaged and friended the defendant on MySpace. The court concluded that the defendant was entitled to a new trial because bias must be presumed given the circumstance.

Lastly, there are ethical considerations that should be taken to account with concern to judges. According to ABA Formal Opinion 462, the use of social media by judges "must comply with the relevant provisions of the Code of Judicial Conduct and avoid any conduct that would undermine the judge's independence, integrity, or impartiality, or create an appearance of impropriety" (ABA Committee on Ethics & Professional Responsibility, Formal Opinion 462 (2013); c.f. Brower et al., 2013, p. 10). Attorneys should avoid "friending" judges that they may have to appear before to avoid creating possible reasons for recusal. Social media brings with it ethical concerns for all the parties that are involved in the courtroom.

Despite the strong consensus of the admissibility of social media in general, limitations do exist within these sources. For instance, the review of the terms of use by Trasatti and Horevay was conducted in 2013. It is reasonable to question whether or not the terms of use have changed significantly in the last four years. It is also important to consider that Facebook and MySpace may not be representative of all social media websites. Additionally, in his article, Gensler (2012) limits his analysis to the Federal Rules of Civil Procedure because the discovery scheme it lays out it purposefully vague. However, the impact of the FRCP on the discoverability of social media could have been better exemplified by including case law and judicial precedent.

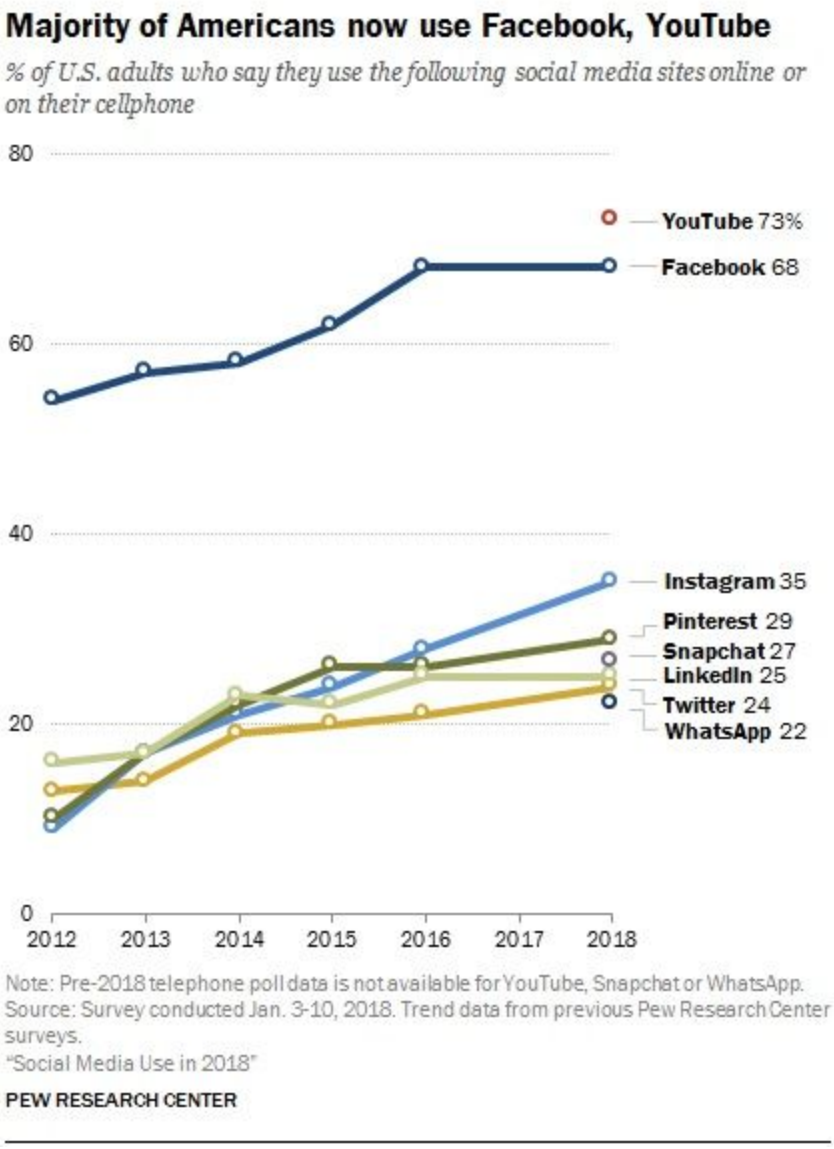
While authors such as Brower et. al, Trasatti and Horevay strongly agree on the usefulness of social media as a source of evidence, limitations exist within these sources. The validity of the Pew Research center survey provided by Trasatti and Horevay (2013) could be called into question as the method used for gathering the statistics is unknown. The statistics pulled from this survey are from late 2012. The survey does not suggest a trend and these numbers may have shifted significantly in the last five years. Next, Moore (2014) did not conduct a survey concerning the way internet users utilize social media. Readers must trust the validity of the sources that were pulled from to draw such conclusions.

While literature demonstrates a strong agreement concerning ethics, limitations do exist within these sources. Keefe (2017) is overly reliant on state level ethics opinions for her conclusions. The opinions of individuals involved with the American Bar Association or the ABA itself are not included within the conclusions. Next, Trasatti and Horevay

(2013) reference a single court case to demonstrate ethical dilemmas concerning the jury, however they do not include similar cases or reference existing ethics opinions on this issue. This is inherently limited and may have been improved by the inclusion of similar case law or researching ethics opinions of the American Bar Association.

Despite how recent the incorporation of social media into the legal system has been, an accord is present about the applicability of evidence gathered from social media websites, the serviceability of social media in the search for the truth, and the responsibility of courtroom participants given the most ethical use of social media. Research shows that most of the content that users share on their personal social media accounts is generally discoverable when the motion for discovery is tailored to include posts that are pertinent to the given court case. Additionally, case law has demonstrated that social media content is just as admissible as any other relevant document despite the user's reasonable expectation of privacy. Furthermore, the probative value of social media evidence has proven to be an evidentiary treasure-trove to the legal community. Lastly, the legal community has shown agreement on the most ethical use of social media by witnesses, jurors, attorneys, and judges. The current state of research on this topic does not address the effectiveness of preemptively deleting social media accounts in anticipation of a lawsuit.

III. PERVASIVE USE AND ACCESSIBILITY



Social media is any kind of forum on the internet which allows for users to communicate and interact with content on the host social media website. According to poll and survey data from the Pew Research Center (2018), more than 55 million adults in America use some form of social media to communicate. It has become increasingly important for networking in the modern world with more than 2 billion users as of 2018. A majority of Americans casually subject themselves to their dopamine-driven feedback loop that drive Facebook usage. Much the same as gambling addiction, social media platforms are highly addictive. Speaking on the Dangers of Social Media Addiction, Simon Sinek (2017) has said, "We know that engagement with social media and our cellphones releases a chemical called dopamine. That's why when you get a text, it feels good...It's why we count the likes. It's why we go back ten times to see if [there is a notification]. It's why we keep going back to it. Dopamine is the exact same chemical that makes us feel good when we smoke, when we drink, and when we gamble. In other words, it's highly, highly, addictive." About 73% of people claim to have experienced a mild state of panic in the event of misplacing their smartphone. Social media fills up our spare moments and provides a source of instant gratification (Sinek 2017).

Users build profiles about their lives which help them to share information and pictures that are important to them (Barnum, 2014). It allows for them to develop online communities centered around their interests with relative ease and incomparable efficiency. Once an individual has cultivated a social media profile, they can begin to search for other users by searching for a name, email address, hometown, etc. However, users are not limited to searching for others by known information. Social media websites

allow for group formations around specific interests. For example, a college student may search for a Facebook group for their specific university class.

A privacy component is present given that users can select which information is shared and which information is not shared. By opting for privacy settings, the user may decide to make their profile viewable to only approved individuals or they could use privacy settings to limit content to specific individuals or group of individuals. These settings will limit what type of information is accessible to the public in general (Keefe, 2017). Differing opinions exist on how social media posts could be considered private when the number of connections an individual has would otherwise be regarded as a public forum. For example, consider whether or not an individual who shares information in front of 100+ individuals in an auditorium should reasonably expect to have that information to remain "private." Contrast that to sharing the same information to 100+ followers on a social media platform. Additionally, followers on websites such as Facebook, Twitter, and Tumblr have the ability to share social media posts. That would mean that the original social media user may not be connected directly to others who will view their text posts, vacation photos, or blog links.

Considering the widespread use of social media websites and its networking potential, dually considered should be its relevance and impact on courtroom procedures. What type of posts can be retrieved from these social media websites is governed by the Stored Communications Act (Medina, 2013). This act was codified as part of the Electronics Communications Act at 18 U.S.C. Chapter 121 §§ 2701–2712. It directs the procedure to be followed for the voluntary and compelled disclosure of "stored wire and

electronic communications and transactional records" held by third-party internet service providers (ISPs). It is common for individuals to not restrict their social media posts. They may not opt-in for privacy settings for text posts and photos because they feel completely comfortable sharing with friends and family. It is also helpful for networking purposes if they can be found and content can be referenced to double check that they are indeed a specific person. For this reason and others, much of the existing content on sites like Twitter, Facebook, Instagram is publically accessible. This is really good news for litigation. Information found on the publically accessible portion of social media pages can be freely obtained like any other public record, e.g. court documents, police reports, etc.

Many courts interpret the law as creating a right to privacy for individuals in stored communications that are not intended to be public. As a result, courts may not require social media sites to hand over information contained on a user's personal site pursuant to a subpoena. Accordingly, if you subpoena the social media site to provide the information and they refuse to do so, you may be able to obtain a court order to require the adverse party to sign a consent form that can be attached to the subpoena. This would essentially then give the social media site "consent" of the user to turn over the information.

IV. SOCIAL MEDIA CONTENT

Social media platforms have grown more and more rapidly after their emergence in the early 2000s. With social media giants such as Facebook, Twitter, Instagram, and Snapchat popping up in the following decade, the web has become inundated with personal information. One of the problems that has surfaced in the wake of this development is user privacy. Given the advancements in social technologies, differing levels of privacy exist for the protection of individual content. There are a couple ways to classify the different levels of social media privacy. Public social media content is content which is generally accessible from a quick search of the internet. Private social media content is usually filtered by some layer of setting preference. Ephemeral social media content is information that is collected when people take surveys, play games, or respond to polls (Moore, 2014).

Social media profiles are user generated. Users typically share information in order to connect to their friend networks. They often share their daily routines, preferences, and details about their interpersonal relationships (Moore 2014). Publically accessible social media content is most likely to be entered into evidence. It is treated as any other form of evidence which may be gathered in preparation for a trial. Anyone can

get on the web and search for the social media of another person. As long as privacy settings are not being applied to the content and account, then the results of the search will reveal whatever the user has revealed about themselves. Different social networking sites tend to prompt different types of content being posted. Additionally, different people will decide to post different types of content or even limit what they decide to share. Depending on who is the witness, defendant, or plaintiff in question, they may or may not have tractionable evidence posted. If a prosecutor is searching for character evidence to make a point, there is no guarantee that the content that surfaces will be actionable. Consider how some users will decide not to share photos of their lives, but rather will decide to share funny cat videos or memes. A meme is a "humorous image, video, piece of text, etc., that is copied (often with slight variations) and spread rapidly by Internet users." Depending on the facts and circumstances of the case, a meme may or may not be relevant to prove a component of a case.

While public web forums such as the Facebook wall or Twitter feed are evidently more public, when it comes direct messages to another individual, one might expect a greater amount of privacy. The standard rules of evidence generally apply, Facebook messages may be entered into evidence by an authenticating witness if it was a conversation between themselves and another. In *Smith v. State*, 136 So. 3d 424 (Miss. 2014), "Smith objected to the admission of the Facebook messages into evidence as hearsay and as not being properly authenticated." Smith was convicted for the murder of his seventeen-month-old stepchild Ally. Jenny Waldrop, mother of Ally and younger sibling Ethan, helped authenticate the messages by her testimony. The necessary

questions that should be asked to authenticate evidence can be seen in this excerpt from *Smith v. State.* The attorney on direct examination establishes that there are Facebook messages between the Waldrop and Smith. The attorney shows counsel opposite the Facebook messages and then asks to approach the witness. The attorney asks the witness to identify to exhibit, explain their familiarity with the exhibit, establish same condition, and finally asking the court to enter the exhibit into evidence. The prosecutors authenticated the Facebook messages by using this line of questioning: "Q: Did he — did he give you indications in your Facebook discussions or letters, that he wanted it to be just the three of you, you, Ethan, and him, and not Ally? Q: Did he indicate to you in those communications that he felt like he was, for a lack of a better term, about to boil over with anger? Q: Jenny, I am going to show you copies of three documents, and I want you to look at these and tell me if you can identify what they are. Q: It's Page 1 — it's three pages. What is the second page?"

One of the messages from Smith read "[I] feel my temper building and [I] know [I] will hurt someone, they are playing with fire and have no clue." The trial court overruled Scott Smith's objection. The Facebook messages were entered into evidence. Next, the case went to the Court of Appeals to determine whether the Facebook messages would be considered inadmissible hearsay or insufficiently authenticated. The Mississippi Supreme Court granted a Writ of Certiorari, however they found no reversible error. Scott Smith was convicted of capital murder for the death Ally Waldrop.

In *Smith,* the court described what sufficient authentication of Facebook messages consists of. The situations include: "the sender admits authorship, the purported sender is

seen composing the communication, business records of an internet service provider or cell phone company show that the communication originated from the purported sender's personal computer or cell phone under circumstances in which it is reasonable to believe that only the purported sender would have access to the computer or cell phone, the communication contains information that only the purported sender could be expected to know, the purported sender responds to an exchange in such a way as to indicate circumstantially that he was in fact the author of the communication, or other circumstances peculiar to the particular case may suffice to establish a prima facie showing of authenticity." The list of situations is not meant to be exhaustive, but to demonstrate an array of circumstances in which authentication has occurred in line with the Mississippi Rule of Evidence 901. Mississippi Rule of Evidence 901(a) states that "[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." *Todd v. State*, 806 So.2d 1086 (Miss.2001). Emails and letters were in question in *Kearley v. State,* 843 So.2d 66 (Miss. 2002), for which the court ruled to be properly authenticated for the correspondences and admissible. They email and letters were what they purported to be.

In the case of *Boyd v. State*, 175 So. 3d 1, thirty-two-year-old Tyrone Boyd was found guilty under Mississippi Code Section 97-5-33(6) for the exploitation of a twelve-year-old child. On appeal, Boyd claimed that the court erred when Facebook and text message printouts were entered into evidence. Boyd asserted that the prosecution failed to properly authenticate the documents. The Mississippi Rule of Evidence Rule

901(a) informs us that before evidence can be admitted, it must be authenticated and identified. This authentication should demonstrate that "a matter is what its proponent claims it to be." M.R.E. 901. The court found that Boyd did not object when it was entered at trial and that his claim was meritless. Boyd tried to assert that he had not authored the messages but did not offer a reason why the messages would have been authored by anyone else. His conviction was affirmed and he was sentenced for exploitation of a child.

V. EXPECTATIONS OF PRIVACY

The expectation of privacy for communications has long been established in the law. From the time of the bootleggers, the 1928 decision in *Olmstead v. United States* gave all U.S. citizens a reasonable expectation of privacy in their telecommunications. The federal agents investigating Roy Olmstead used existing technology to listen in on his phone conversations. They suspected of violating the National Prohibition Act. The petitioners took issue with the warrantless tapping of phone lines. The court agreed that without judicial approval, the tapping of phones was a violation of their fourth and fifth amendment rights. This case refined the law created by cases like *Olmstead* and *Goldman v. United States.* The latter case was ruled on in 1942 which ruled that investigators did not violate the fourth amendment with the use of a dictaphone recording from the other side of a wall of an adjoining room. A reasonable expectation of privacy was established. It was a significant leap forward which protected intangible communications. Some thirty nine years later, *Katz v. United States*, 389 U.S. 347 (1967) applied the Fourth Amendment concept of the "unreasonable search and seizure" to intangible communications. This has set the precedent that is currently unfolding in the form of case

law, which has left the door open for individual jurisdictions to decide what is a "reasonable expectation of privacy."

The former president of the Ohio Association of Criminal Defense Attorneys remarked on the usefulness of social media in saying that "I personally have been involved in several trials where credibility was completely lost in a matter of seconds when the witness was presented with something inconsistent they had written in the past" (Callahan 2012). The types of data which gets shared everyday on social media sites includes a variety of information, such as biographical information, pictures, and life updates. Information gleaned from social media profiles can inform the court about a litigant's behavior and activities. It is especially helpful to highlight contradictions in testimony thereby diminishing their credibility. The Federal Rules of Civil Procedure allows for the discovery of all relevant information so long as it is not a privileged communication, such as between a doctor and a patient, married couples, and therapist and patient. Fourth Amendment law is most relevant to accessing the admissibility of social media outside of authenticating witnesses.

Outside of the courtroom, law enforcement must balance individual privacy and public safety (Curphey, 2005). Expectations of privacy are not merely at issue in ongoing court cases. At times, the prosecutor may decide to monitor internet activity while they are building a case against an individual or entity. The courts will determine whether the individual's expectation of privacy or the government's interest in skipping the standard procedure of getting "a warrant or some level of individualized suspicion" carries greater weight. *Nat'l Treasury Employees Union v. Von Raab,* 489 U.S. 656, 665-66 (1989).

Probationers were at issue in the Second Circuit case *United States v. Lifshitz,* 369 F.3d 173, 193 (2d Cir. 2004). It held that broadly monitoring the computer activities of probationers was out of step with the Fourth Amendment. It is difficult to justify monitoring probationers when there is no reason to suspect them of acting in bad faith. The *Lifshitz* opinion provides the government a procedure to step around the Fourth Amendment protection when it would be impractical to do so as a result of "special needs, beyond the normal need for law enforcement." *T.L.O.,* 469 U.S. at 351. Otherwise, when the state begins to monitor computer activities without a warrant, they have infringed on the rights of citizens. Social media sites have mostly been held to be public platforms to the point of limiting Fourth Amendment protection, such as in *United States v. Meregildo*, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012). The *Meregildo* court held that Facebook posts are not protected because of their public nature. As long as investigators do not aim to obtain broad swaths of information, they are generally in the clear. A warrant to search a Facebook account is not considered a "general search" when it is "narrowly tailored to the aim of the investigation." The court was able to defend its inquiry because determining who the defendant had contact with was relevant to determining whether he had attempted to join a terrorist group.

VI. Stored Communications Act

Codified in 1986, the Stored Communications Act (SCA) was first applied to Facebook by a California district court in 2010. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010). Highlighting SCA, 18 U.S.C. 2701, the court ruled that the government does not have the power to compel Internet Service Providers to "disclose information in their possession about their customers and subscribers." The SCA prevents an obligation of a ISP to respond to a civil subpoena. A litigant should request the content directly from the adverse party. In *Romano v. Steelcase,* the New York trial court allowed complete discovery of the plaintiff's current and historical Facebook and MySpace pages. It was a significant precedent because the court discarded the idea that privacy settings should limit discovery. The court decided this way due to the fact that litigants are unable to reasonably rely on Facebook's privacy settings to bar discovery of information they did not intend to share through the site. Self-regulated privacy settings give parties anticipating lawsuits the chance to limit discovery, which the court decided against.

Other courts have chosen to approach this dilemma by opting for "in-camera review." This is when a judge privately reviews confidential, sensitive, or private information to come to a conclusion about which information is justifiably admissible. The Connecticut district court in *Bass v. Miss Porter's School* decided on this method. The judge reviewed information the plaintiff wished to exclude from discovery. The court rejected the plaintiff's request to limit discovery finding no meaningful distinction between the content the plaintiff had agreed to produce and the content the plaintiff deemed irrelevant. In *Offenback v. Bowman, Inc.,* a district court in Pennsylvania also chose to undergo an in camera inspection. The court did limit the scope of discovery to the information relevant to the personal injury lawsuit.

Some courts require litigants to qualify the request for social media content by establishing relevance first. This is what the circumstances were in the case of *McCann v. Harleysville Insurance Company of New York.* The plaintiff was not required to disclose photographs from her Facebook profile because the defense counsel did not establish that evidence would be relevant (Brown, 2012). In *Piccolo v. Paterson,* the Pennsylvanian court found that the mere possession of a social media page was not enough to compel a search of that Facebook account. The factual predicate was not established to show relevance of obtaining additional photos from the plaintiff's Facebook page. The plaintiff had already turned over pictures of her facial scarring before and after, and the request for her to accept a "friend request" from the defense counsel was deemed "unduly burdensome." Litigants should establish relevance in order for courts to find the information to be discoverable.

Access to social media content has a tendency to hinge admissibility. The content cannot be privileged and must be relevant the facts and circumstances of case at hand. Privacy settings have limited effectiveness in many jurisdictions, due to the broad discovery of admissible evidence permitted by the Federal Rules of Civil Procedure. The two most common ways in which the SCA is violated are: (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system. (18 U.S. Code Section 2701(a)). Access and authorization must be respected given electronic storage of information.

Social media activity illuminates the life of the user, creating a personal record of their life which they continually update. Additionally, there is a false sense of security created by the use of privacy settings which courts have generally regarded as minimal. A subpoena and a consent form can be used to retrieve data in discovery according to the court in *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.,* 961 F. Supp. 2d 659 (D.N.J. 2013). The *Ehling* court did not require the employee to elucidate the private Facebook post. Rather, the court regarded it as protected under the SCA due to its characteristics as an (1) electronic communication which was (2) transmitted electronically, (3) stored electronically, and (4) was private. “Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo optical system” is considered an “electronic communication” under the SCA. Social media gives users the ability to send and receive

communications via their phones, computers, and tablets. This satisfies the "transmitted electronically" element. Social media sites host the content, which is to say that it has been "stored electronically." The final element to protected information under the SCA is "non-public." The *Ehling* court interpreted the SCA to protect private Facebook content. They stated that the SCA "makes clear that the statute's purpose is to protect information that the communicator took steps to keep private." When a user limits the visibility of posts by using privacy settings, they are considered to have taken those steps to satisfy the final element of stored communications protections.

Facebook Messenger privacy protections can be examined by reading the *Crispin v. Christian Audigier, Inc.,* 717 F. Supp. 2d 965 (C.D. Cal. 2010) court case. The *Crispin* court distinguished between (1) opened, saved messages and (2) unopened messages. Opened, saved messages are the least protected requiring only a subpoena or court order and notice. Unopened, private messages require a valid warrant if they are under 180 days old according to the court. However, messages older than 180 days old are accessible in the same manner as opened, saved messages. Whether the content may be classified as a "remote computing service" or "electronic communications system" is key. Opened, private messages were interpreted to fall under the remote computing services provision, which is a site that allows the public the utility of "computer storage or processing services by means of an electronic communications system." 18 U.S.C. Section 2711(2). Email services in general fall under this protection. Unopened private messages fall under the provision for electronic communication systems when the service provider "provides to users thereof the ability to send or receive wire or electronic

communications." 18 U.S.C. Section 2510(15). The reasoning was that the nature of unopened, private messages was held in "temporary, intermediate storage." 18 U.S.C. Section 2510(17)(A). Under the SCA, service providers are barred from disclosing such information without a valid warrant. These protections are negated in the event that a Facebook "friend further discloses the post (of their own volition)." This may happen by using the "share" function on Facebook, which would lead to the information being more public. Twitter has a similar function where users "retweet" posts they like.

VII. ENTERING SOCIAL MEDIA EVIDENCE

A trial court has a vast amount of discretion in the matter of admitting evidence. The bar for entering social media into evidence is correspondingly low. Many courts will find a print out of a social media page to be genuine if the page merely purports to be that particular individual's page. *Porter v. Quarantillo,* 722 F.3d 94, 97 (2d Cir.2013). In most cases, a document may not be admitted into evidence "unless it is shown to be genuine." *United States v. Maldonado-Rivera,*922 F.2d 934, 957 (2d Cir.1990). Available identifying information includes but is not limited to their profile picture, which is generally a headshot of the individual themselves. Additionally, many social media pages include basic information about where the person works, their employment history, their birthdate, their relationship status, their hometown, and even the city in which they presently reside (Brown, 2012).

Sometimes the opposing counsel will assert that the evidence is not what it purports to be, that this social media page is not verifiably linked to their client. Courts have found that the decision as to whether the evidence is authentic is ultimately determined by the jury in the trial court, although litigators have the right to appeal if they believe a mistake of law has occurred. When deciding whether the district court erred, the attorney should consider whether that the error was harmful and an abuse of

discretion. *U.S. v. Vayner*, 769 F. 3d 125 - Court of Appeals, 2nd Circuit 2014. An abuse of discretion is said to have occured when a court has made a decision based on “an erroneous view of the law or on a clearly erroneous assessment of the evidence, or renders a decision that cannot be located within the range of permissible decisions.” Rule 901 of the Federal Rules of Evidence provides that in order to meet the requirement for authentication, an attorney must provide evidence adequate to bolster an assertion that the evidence is what the attorney asserts it to be. Fed. R. Evid. 901(a). According to *U.S. v Pluta,* 176 F.3d 43, 49 (2d Cir.1999), this element met "if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification." Being that the jurors are the fact-finders, they have the burden of determining whether the evidence is what it is purported to be. *See Sliker,* 751 F.2d at 499. The court in *United States v. Sliker* interpreted Rule 901 to have been purposefully vague. Rule 901 is not meant to"definitively establish the nature or quantum of proof that is required" in order to authenticate evidence such as social media *Id.* at 499. Rather the authentication of evidence will be determined by the facts and circumstances relevant to the purposes for which the evidence has been offered. In *U.S. v. Vayner*, the authentication is said to be a “context-specific determination whether the proof advanced is sufficient to support a finding that the item in question is what its proponent claims it to be.” These examples of case law all point to the fact that "[t]he bar for authentication of evidence is not particularly high." *United States v. Gagliardi,* 506 F.3d 140, 151(2d Cir.2007).

It is clear that jurors have a key role to play. When presenting the evidence to the jury, authentication may be direct or circumstantial. *United States v. Al-Moayad,* 545

F.3d 139, 172 (2d Cir.2008). Usually this may be accomplished through "the testimony of a `witness with knowledge' that `a matter is what it is claimed to be.'" *United States v. Rommy,* 506 F.3d 108, 138 (2d Cir.2007). Moreover, the document can be self-verifying if it contains "distinctive characteristics of the document itself, such as its `[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with the circumstances.'" Fed. R.Evid. 901(b)(4). In the case of *Sliker,* 751 F.2d at 488, the bank records seized from an allegedly fraudulent bank did not require a witness to verify, rather they contained enough definitive characteristics to not be mistaken as anything other than what they purported themselves to be.

Whether the evidence is properly authenticated offered to the jury does not discount the fact that the jury may always determine the true reliability. As one court put it "[a]uthentication of course merely renders [evidence] admissible, leaving the issue of [its] ultimate reliability to the jury." *United States v. Tropeano,*252 F.3d 653, 661(2d Cir.2001). The opposing party will always have the ability to challenge the credibility of any evidence that is properly authenticated. Litigants remain "free to challenge the reliability of the evidence, to minimize its importance, or to argue alternative interpretations of its meaning, but these and similar other challenges go to the *weight* of the evidence—not to its *admissibility." Tin Yat Chin,* 371 F.3d at 38. Social media itself has many definitive characteristics that tie a particular web page to the physical embodiment of the person. The photos they share on social media pages, the shared communications with friends over comments on text-posts, photos, and quiz results, all of these things go to tie a social media page to a particular individual.

VIII. CONCLUSION

Social media websites contain relevant and accessible information. When it comes to the discovery stage of litigation, an attorney has a number of tools to obtain documented conversations, text-posts, photographs, and comments. The emergence of social networking websites has resulted in a whole new source of evidence for litigators. The information shared on websites, such as Facebook, Instagram, LinkedIn and Twitter, is within the scope of discovery. However, jurisdictions do vary in terms of scope and the extent to which privacy may be infringed. For example, the degree to which a reasonable expectation of privacy is present.

Americans are documenting their lives online in a way that can be used to demonstrate their offline character. The existence of websites which store personal information has been an emerging development, one which is easily integrated into existing legal frameworks. The Federal Rules of Evidence have not restricted appropriate evidence by the origin of such information. This means that so long as the evidence is not objectionable, it is typically admissible. Social media evidence is treated in a similar manner to physical evidence, public records, and witness testimony. In fact, social media evidence is often authenticated by someone who has been in correspondence with the party. Other times, the social media post in question has not been restricted using privacy

settings. There is reason to believe that social media sites are at the forefront of how Americans interact with their friends, colleagues, and loved ones. When a user checks their social media page, they often confirm their expectations that they have notifications waiting to be checked. To a certain degree, these updates feel equivalent to a successful social interaction. Beyond asking why it is that Americans enjoy this form of online socialization, it is certain that the information shared online may find its way into a courtroom one way or another. It is important for those who choose to participate in maintaining an online presence to beware of the flimsy expectation of privacy associated with social media sites. Discretion should always be exercised before posting sensitive information to public forums. Given the long arm of the legal system, perhaps some opinions, photos, and interactions are best left offline.

List of References

Barnum, E. (2014). *Privacy, social media, and the American workplace: Employment litigation
will never be the same.* Retrieved from: https://www.americanbar.org/content/dam/aba/events/labor_law/am/2014/10a_barnum.au Thcheckdam.pdf

Big Surge in Social Networking Evidence Says Survey of Nation's Top Divorce Lawyers. *American Academy of Matrimonial Lawyers.* (2010).

Brower, S., Longo, A., & Lynn III, C. (2013, August). *Social media evidence: How to find it and
how to use it.* Paper presented at the meeting of American Bar Association, San Francisco, CA.

Brown, K. (2012). *The Risks of Taking Facebook at Face Value: Why the Psychology of Social Networking Should Influence the Evidentiary Relevance of Facebook Photographs.*

Callahan, D. (2012). *Social media posts admissible in court.* Journal-News.

"Crispin v. Christian Audigier, Inc.: Stored Communications Act Protects Facebook and MySpace Users' Private Communications." *Harvard Journal of Law & Technology*, 11 June 2010, jolt.law.harvard.edu/digest/crispin-v-christian-audigier-inc.

Curphey, S. (2005). United States v. Lifshitz: Warrantless Computer Monitoring and the Fourth Amendment. *Loyola Marymount University and Loyola Law School.*

Deibert, Ronald. (2019). The Road to Digital Unfreedom: Three Painful Truths About Social Media. *Johns Hopkins University Press.*

Gensler, S. (2012). Special rules for social media discovery. *Arkansas Law Review*, *65*(1), 7-38.

Haynes, Trevor. “Dopamine, Smartphones & You: A Battle for Your Time.” *Science in the News*, 30 Apr. 2018, sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time/.

Keefe, N. (2017). Dance like no one is watching, post like everyone is: The accessibility of "private" social media content in civil litigation. *Vanderbilt University, School of Law, 19*(4), 1027-1054.

Lange, Chris. (2019). *24/7 wall st.: What merrill lynch sees as the major social media trends in 2019* Chatham: Newstex.

Lederman, Leandra, "Precedent Lost: Why Encourage Settlement, and Why Permit Non-party Involvement in Settlements?" (1999). Articles by Maurer Faculty. Paper 549.

Maerowitz, M., & Mauet, T. (2013). *Fundamentals of Litigation for Paralegals*. Netherlands: Wolters Kluwer Law & Business.

Medina, Melissa. "The Stored Communications Act: An Old Statute for Modern Times."*American University Law Review*, vol. 63, no. 1, 2013, pp. 267.

Moore, J. (2014). Social-media discovery: It's a matter of proportion. *Thomas M. Cooley Law Review, 31*(3), 403-427.

Sinek, S. “Simon Sinek, The Dangers Of Social Media Addiction.” *YouTube*, YouTube, 30 Mar. 2017, www.youtube.com/watch?v=YPmNf362_K0&t=932s.

Smith, A., Anderson, M. (2018). Social Media Use in 2018. *Pew Research Center: Internet & Technology.*

Trasatti, M., Horevay, A. (2013). Litigation and social media: Using social media to your advantage at every step of the trial. *Federation of Defense and Corporate Counsel, 63*(4), 252-278.

Yurtoğlu, Nadir. "Smartphone Restriction, Withdrawal Symptoms." *History Studies International Journal of History*, vol. 10, no. 7, 2017, pp. 241–264., doi:10.9737/hist.2018.658.

Case law:

Bass v. Miss Porter's School, 738 F.Supp.2d 307 (2010)

Boyd v. State, 175 So. 3d 1

Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010)

Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 961 F. Supp. 2d 659 (D.N.J. 2013)

Katz v. United States, 389 U.S. 347 (1967)

Kearley v. State, 843 So.2d 66 (Miss. 2002)

McCann v. Harleysville Insurance Company of New York, No. 10-00612, 1179 (N.Y.A.D. 4 Dept. Nov. 12, 2010)

Piccolo v. Paterson, No. 2009-4979 (Pa. C.P. Bucks May 6, 2011)

Porter v. Quarantillo, 722 F.3d 94, 97 (2d Cir.2013)

Romano v. Steelcase Inc., 907 N.Y.S.2d 650 (2010)

Offenback v. L.M. Bowman, Inc., No. 1:10-CV-1789 (M.D. Pa. 2011)

Olmstead v. United States, 277 U.S. 438 (1928)

Smith v. State, 136 So. 3d 424 (Miss. 2014)

State of West Virginia v. Dellinger, Case No. 35273 (Va.Ct. App. June 3, 2010)

Stored Communications Act 18 U.S. Code Section 1701

T.L.O., 469 U.S. at 351.

Todd v. State, 806 So.2d 1086 (Miss.2001)

United States v. Al-Moayad, 545 F.3d 139, 172 (2d Cir.2008)

United States v. Gagliardi, 506 F.3d 140, 151(2d Cir.2007)

United States v. Lifshitz, 369 F.3d 173, 193 (2d Cir. 2004)

*United States v. Maldonado-Rivera,*922 F.2d 934, 957 (2d Cir.1990)

United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012)

United States v. Pluta, 176 F.3d 43, 49 (2d Cir.1999)

United States v. Rommy, 506 F.3d 108, 138 (2d Cir.2007)

United States v. Sliker, 942 F2d 795 (1991)

United States v. Tin Yat Chin, 371 F.3d 31 (2d Cir.2004)

United States v. Tropeano, 252 F.3d 653, 661(2d Cir.2001)

United States v. Vayner, 769 F. 3d 125 - Court of Appeals, 2nd Circuit 2014

Appendix I

Statutory law affecting stored communications includes:

1. The Federal Trade Commission Act (FTC Act), 15 U.S. C. § 25, (mostly prohibits "unfair and deceptive practices affecting commerce"). Federal Communications Commission (FCC) was established to regulate "interstate and foreign communication by radio, telephone, telegraph, and television." The FTC has filed suit using this statute in cases in which the company failed abide by their own privacy policy. Generally, there are two types of legal action taken by the commission:

(1) "where the company promised a specific level of data security to its customers, only to have its data compromised because it did not in fact deliver the promised level of security," and;

(2) "where the company promised not to sell or otherwise disclose customer information to third parties, only to do so when a sale of the information turned out to be financially attractive to the company";

2. The Financial Services Modernization Act, also known as the GrammLeach Bliley Act (GLBA), 15U.S.C. §§ 6801-6809, protects customers of financial institutions by

requiring privacy notices be sent out. These notices would provide customers with the ability to opt-out of disclosing their financial information with third-parties;

3. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), supports the use of electronic transactions. It utilizes an opt-in framework regarding sensitive health information;

4. The Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-08 and 16 C.F.R. Part 312, designed to protect and regulate information about children under the age of 13;

5. The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34 C.F.R. § 99, and the Protection of Pupil Rights Amendment (PPRA),"), 20 U.S.C. § 1232h and 34 C.F.R. § 98, designed to protect and govern student information. The federal funding of institutions is contingent upon FERPA compliance. It covers both public and private institutions who "provide education services or instruction." See 34 C.F.R. § 99.3.

6. The Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681 et seq., consumer reporting agencies and the data they collect is governed by this statute;

7. Stored Communications Act (SCA), 18 USC §§ 2707-2711, which is part of the Electronic Communications Privacy Act, it the statute which most greatly affects the discovery of social media evidence. The SCA was enacted in 1986, which makes it a pre-Internet statute.

Appendix II

Examples of social media sites: Ashley Madison, Baidu Tieba, Bumble, ChristianMingle, Facebook, FarmersOnly, Flickr, Friendster, Foursquare, Grindr, Google+, italki, Instagram, Jiepang, LINE, LinkedIn, MyHeritage, Myspace, Pinterest, QQ, Qzone, Quora, Reddit, Vampirefreaks, GroupMe, Skype, SnapChat, Telegram, TikTok, Tindr, Tumblr, Twitter,VKontakte (VK), Viber, Vine, WeChat, Weibo, We Heart It, Youtube