Uploading Guilt: Adding a Virtual Records Exception to the Federal Rules of Evidence Note

Allison L. Pannozzo

Follow this and additional works at: https://opencommons.uconn.edu/law_review

Recommended Citation
https://opencommons.uconn.edu/law_review/170
Note

UPLOADING GUILT: ADDING A VIRTUAL RECORDS EXCEPTION TO THE FEDERAL RULES OF EVIDENCE

ALLISON L. PANNOZZO

The creation of email and social networking websites significantly altered the practice of law. The wealth of information exchanged through emails, and postings on Facebook and MySpace has aided prosecutors, defense attorneys, and civil trial attorneys in litigating their cases. But despite the prevalence of email and social networking evidence in the legal field, the Federal Rules of Evidence have remained inadequate for dealing with this type of technology. Attorneys have been met with mixed results in their attempts to authenticate emails and social networking evidence at trial.

Currently, courts are split on whether the content should even be admitted. Some courts take a hard-line approach, finding email and social networking content inherently untrustworthy. Others find that the content is not any different than signatures and letters, which have the potential to be forged. Those courts that find the content suitable are not in agreement over the need for a new Federal Rule of Evidence.

This Note argues that email and social networking evidence should be admitted in both criminal and civil court cases, given courts’ long history of admitting circumstantial evidence in trials. It further proposes an amendment to the Federal Rules of Evidence regarding virtual records. Such a rule, modeled after the public records exception, is appropriate in recognition of the fact that new technologies have made it easier for individuals to securely maintain private records, such as emails, bank statements, and social networking posts on virtual databases.
I. INTRODUCTION ................................................................. 1697

II. THE EMAIL AND SOCIAL NETWORKING ERA ................. 1699
   A. EMAIL: THE INTERNET’S ONE TRUE “KILLER APP” ............. 1699
   B. THE RISE OF SOCIAL NETWORKING WEBSITES .................. 1699

III. EVIDENTIARY PROBLEMS WITH EMAIL
     AND SOCIAL NETWORKING SITES ...................................... 1701
   A. DISCOVERABILITY VS. ADMISSIBILITY ............................. 1701
   B. THE RELEVANCY REQUIREMENT ...................................... 1702
   C. THE HEARSAY HURDLE .................................................. 1704
   D. BEST EVIDENCE RULE .................................................. 1707

IV. THE MYRIAD WAYS TO PROVE ATTRIBUTION
    UNDER THE CURRENT RULES ............................................. 1708
   A. THE MANY METHODS OF AUTHENTICATION ......................... 1710
   B. PROBLEMS WITH SELF-AUTHENTICATION ............................ 1713

V. THE ADVISORY COMMITTEE SHOULD ADD
    A “VIRTUAL RECORDS” EXCEPTION TO
    THE FEDERAL RULES OF EVIDENCE .................................... 1715
   A. PROPOSED VIRTUAL RECORDS RULE 901(b)(11) .................. 1716

VI. IMPLICATIONS OF USING EMAIL
    AND SOCIAL NETWORKING EVIDENCE
    IN THE LEGAL PROFESSION ............................................. 1719

VII. CONCLUSION .................................................................... 1722
UPLOADING GUILT: ADDING A VIRTUAL RECORDS EXCEPTION TO THE FEDERAL RULES OF EVIDENCE

ALLISON L. PANNOZZO

The social media has become more than just social. It has for many... become a part of [a] way of life. Tweeting, texting and e-mails have not only replaced, to some extent, face to face social intercourse but also have changed the way business and even the practice of law is conducted.¹

I. INTRODUCTION

We live in an age when telephone calls are replaced by text messages, people find their soul mates through a computerized “matchmaker,” bills can be paid by a click of a computer mouse, and sending a birthday greeting is as easy as posting on one’s Facebook “wall.” Lawyers, judges, and legal scholars have had great difficulty dealing with these technological advances.² And although many have acknowledged the effects of social media on the practice of law, the Federal Rules of Evidence (“Rules”) have failed to do so.

To be fair, the original authors of the Rules could not possibly have imagined how much of today’s law practice would be conducted electronically. But such limited foresight has left the Rules inadequately prepared to deal with the advances in technology.³ The common law rules

² See Lyria Bennett Moses, Recurring Dilemmas: The Law’s Race to Keep Up with Technological Change, 2007 U. ILL. J.L. TECH. & POL’Y 239, 239–40 (2007) (“When computers took over important business functions... lawyers pondered over how computers would be classified by judges. They asked what the consequences might be of treating a computer as a legal entity, whether computer printouts ought to be admissible as evidence in court, whether data stored in a computer might constitute a writing for the purposes of the Statute of Frauds and the Statute of Wills... among other questions.”) (citations omitted).
³ See Evelyn D. Kousoubris, Computer Animation: Creativity in the Courtroom, 14 TEMP. ENVTL. L. & TECH. J. 257, 261–62 (1995) (discussing the adaptability of the Rules to new technologies); Moses, supra note 2, at 241 (“The tension between law and technology has been observed by multiple authors and is often reflected in metaphors involving competitors in a race with law the inevitable loser.”).
were amended to include presentation media in the forms of mechanical and
electronic recordings, x-ray machines, motion pictures, and
photography; however, "the vague statutory language of the amended
Rules has created ambiguity as to the admissibility of new technologies." For
example, even after the Rules were amended to include presentation
media, Congress had to alter the definition of photographs to specifically
include videotapes. Based on this history of evidentiary policy, in which
evolution comes slowly, it should be no surprise that social networking
websites ("SNS") and emails currently present significant evidentiary
problems. The problems will continue to grow as SNS and emails
completely replace letter writing, telephone calls, and personal diary
entries.

SNS pose evidentiary problems in a number of areas, including
authentication, relevancy, hearsay, and best evidence issues. Currently,
courts are split on how to handle email and SNS content. Those courts that
feel the content should be admitted also believe that the current Rules
adequately address evidentiary problems. Although this approach may
work for relevancy, hearsay, and best evidence issues, authentication poses
a much larger problem, since attribution may be difficult to prove.

This Note argues for a new authentication exception regarding virtual
records. It asserts that content from emails and SNS should be admitted
into evidence at court trials, as circumstantial evidence is routinely
admitted at trials and has formed the basis for many verdicts. Part II traces
the history of email and SNS. Part III discusses relevancy, hearsay, and
best evidence issues, and demonstrates how courts have thus far applied
the current Rules to email and SNS evidence. Part IV identifies the
problems with the current authentication methods for email and SNS
evidence. Part V proposes an amendment to the Rules regarding virtual
records. Finally, Part VI discusses the implications of allowing email and
SNS evidence into the courtroom.

4 Kousoubrias, supra note 3, at 261.
5 Jonathan D. Kissane-Gaisford, Note, The Case for Disc-Based Litigation: Technology and the
6 See id. (noting that, given the Rule's "rough track record," it was not a surprise that disc-based
litigation posed significant challenges to the evidentiary process, and that such challenges "will not be
overcome easily through individual and haphazard interpretations").
7 Courts have begun to recognize the prevalence of electronic evidence and are attempting to
figure out the problems with admissibility. See, e.g., Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534,
585 (D. Md. 2007) (stating that it can be expected that "electronic evidence will constitute much, if not
most, of the evidence used in future motions practice or at trial").
8 See In re F.P., 878 A.2d 91, 95 (Pa. Super. Ct. 2005) ("Essentially, appellant would have us
create a whole new body of law just to deal with emails or instant messages . . . . We believe that e-
mail messages and similar forms of electronic communication can be properly authenticated within the
existing framework of [the state's rules of evidence].")
II. THE EMAIL AND SOCIAL NETWORKING ERA

A. Email: The Internet’s One True “Killer App”

Many people believe that email is a 1990s technology; however, Ray Tomlinson is credited with sending the first email between computers in 1971. In 1976, Jimmy Carter utilized email for his presidential campaign and Queen Elizabeth of England sent her first email across the Atlantic. Though the Internet has many uses, from educational enrichment to shopping and entertainment, its one true “killer app” is email.

According to an August 2011 survey by Pew Research Center, ninety-one percent of adult Internet users send or read email. The Radicati Group’s study on internet usage estimated that a total of 247 billion email messages were sent per day in 2009 and expects the figure to almost double to 507 billion messages sent per day by 2013. It is no surprise, then, that email has almost completely replaced letter writing in both the public sector and the business world.

The overwhelming use of email contributes to this Note’s argument that the Rules are outdated and must respond to the problems regarding this type of evidence.

B. The Rise of Social Networking Websites

Professors danah boyd and Nicole Ellison define a social network as an Internet service that allows a person to create a public or “semi-public” profile on a system, and gather and access a list of other subscribers with whom they share an interest. There are hundreds of SNSs. Each website facilitates different interests and goals. While some seek to help strangers connect based on shared social values or hobbies, others cater to
those who share political views, religious belief, or sexual identity. The first SNS, “SixDegrees,” launched in 1997, and laid the groundwork for the social networking phenomenon. Today, the most popular sites, and those that will be the main focus of this Note, are MySpace and Facebook.

1. MySpace

Tom Anderson and Chris DeWolfe created MySpace in 2003. Initially, MySpace served as a means for local bands and club owners to post information and become “friends” with fans. The site then became the “online equivalent of your high school lunchroom, your college quad, your favorite bar;” users create and decorate their own profiles, upload music and video clips, post photographs, author blogs, play games, and chat with friends in real time.

2. Facebook

Facebook, a site similar to MySpace, emerged at Harvard University in January of 2004. Mark Zuckerberg, inspired by a bound version of his classmate’s orientation photographs, devoted his January break to creating a site that catered to his college community. Facebook quickly gained popularity and expanded to Columbia, Stanford, and Yale in February of 2004. As Facebook opened to other schools, members were required to have university e-mail addresses in order to preserve the site’s “intimate”

18 Id.; see also, e.g., 20DC, http://www.20dc.com/ (last visited Apr. 5, 2012) (“20DC is an all-partisan political social network that allows citizens to connect with politicians, candidates and each other to organize and take action.”); BLESSEDIT, http://www.blessedit.com (last visited Apr. 5, 2012) (“[B]lessedit.com is a social bookmarking site from a Christian perspective.”); GLBSOCIAL, http://www.glbsocial.net (last visited Apr. 5, 2012) (catering to the gay, lesbian and bi-sexual social network).

19 See Jill Kelley, AOL, SixDegrees.com Built Road to Facebook, DAYTON DAILY NEWS, May 1, 2009, at D7 (“SixDegrees allowed its users to create profiles, invite friends, organize groups and surf other user profiles. Although that site only lasted a few years, it left its mark on the cyberworld, offering a platform for similar sites.”).

20 Pew Internet: Social Networking, PEW INTERNET (Mar. 29, 2012), http://pewinternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx (finding that ninety-two percent of SNS users are on Facebook, and that MySpace is the second most used site with twenty-nine percent of SNS users owning a profile).

21 Patricia Sellers, MySpace Cowboys, FORTUNE, Sept. 4, 2006, at 66, 70.

22 See id. (using friend as a figurative term). One can befriend total strangers on MySpace as evidenced by the fact that creator Tom Anderson befriends every person that creates a profile on the site. He currently has 11,792,611 MySpace “friends.” Tom Anderson, MYSPACE, http://www.myspace.com/tom (last visited Apr. 4, 2012).

23 Sellers, supra note 21, at 68.


25 Id.

26 Id.
setting. Starting in September 2005, the site abandoned its aim to serve a niche demographic, and became available to high school students, corporate professionals, “and, eventually, everyone.” Members can upload photos of themselves and others, post messages on their friends’ profiles, send private messages similar to e-mails, create event invitations, play games, and chat with friends in real time. Similar to MySpace, Facebook frequently adds new features.

Much like the statistics on email, the amount of time people spend on SNS cannot be ignored and supports this Note’s argument that the Rules should be amended to include a virtual records exception. Since January 2012, approximately 40,000 new users have signed up for MySpace per day. Facebook has 845 million users, over fifty percent of whom log onto the site each day. Users spend over 700 billion minutes per month on Facebook.

III. EVIDENTIARY PROBLEMS WITH EMAIL AND SOCIAL NETWORKING SITES

There are a number of circumstances in which a lawyer might want to use emails and information from an individual’s social networking profile at trial. For example, personal injury lawyers for the defense may be especially interested in photographs or status updates which demonstrate that an opponent is not as badly injured as he or she claims. Prosecutors may find the information useful when validating a suspect’s alibi, or linking someone to a crime through communications with other site members. Divorce attorneys may look to the opposing party’s profile for information that could be used in child custody disputes or alimony calculations.

A. Discoverability vs. Admissibility

The discoverability of SNS evidence was once thought to be a novel concept. But, in 2009 the United States District Court for the District of Colorado enforced a subpoena for MySpace and Facebook content

---

27 boyd & Ellison, supra note 16, at 218.
28 Id.
information, noting that “the information . . . is reasonably calculated to lead to the discovery of admissible evidence.” 32 Subsequently, in 2010, the Southern District of Indiana ruled that social networking content is not shielded from discovery simply because it is password protected. In EEOC v. Simply Storage, the court found it “reasonable to expect severe emotional or mental injury to manifest itself in some SNS content.” 33 The court also determined that any profiles, postings, messages, photographs, or videos that “reveal, refer, or relate to any emotion, feeling or mental state . . . or relate to events that could reasonably be expected to produce a significant emotion, feeling, or mental state” must be produced along with any third party communications that “place these claimants’ own communications in context.” 34

While Ledbetter and Simply Storage corrected problems with discoverability, the cases did not discuss or provide guidance on admissibility. 35 It is important to note that “[r]elevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.” 36 While courts have allowed attorneys to look at SNS and email content when preparing for a trial, it does not necessarily follow that courts should, or will, allow attorneys to bring that evidence into court. The evidence must still satisfy relevancy, hearsay, authentication, and best evidence rules to pass at trial. The foregoing sections will discuss relevancy, hearsay, and best evidence issues as applied to the current Rules.

B. The Relevancy Requirement

Based on the Rules’ definition of relevancy—i.e., “any tendency to make a fact more or less probable than it would be without the evidence; and the fact is of consequence in determining the action”— 37 the content of emails and SNS can certainly be relevant and has already aided attorneys during discovery. The problem with such evidence lies with Rule 403’s

33 EEOC v. Simply Storage Mgmt., 270 F.R.D. 430, 435 (S.D. Ind. 2010) (articulating that the content “might reveal whether onset occurred, when, and the degree of distress”).
34 Id. at 436.
35 See id. at 437 (stating that the court’s order “does not preclude objections to admissibility at a later stage or requests”). Furthermore, the court noted that the concern that embarrassing information may be revealed from claimants’ SNS was outweighed by the fact that the production sought was for information that was “already shared with at least one other person through private messages or a larger number of people through postings.” Id. This suggests that privacy concerns may not be a sound basis for excluding evidence at trial because, as the court noted in Simply Storage, “Facebook is not used as a means by which account holders carry on monologues with themselves.” Id. (internal citations and quotations omitted).
36 FED. R. CIV. P. 26(b)(1).
37 FED. R. EVID. 401.
provision that unfairly prejudicial and confusing evidence must be excluded.\(^{38}\) Legal scholars argue that evidence from email and SNS has a greater chance of unfairly prejudicing and misleading a jury. One scholar notes that "the normalcy of expressing contemporaneous observations through . . . social media sites" presents a "unique opportunity" for litigants to create false statements.\(^{39}\) Even when a user does not wish to make a false statement, there is a concern that many people exaggerate in their postings in an effort to obtain "highly socially desirable identities."\(^{40}\) On the other hand, one scholar expressed the concern that the "faux intimacy of social media seduces users into believing that their communications are like hushed confessional."\(^{41}\) Jurors that use social media websites may identify with this "faux intimacy" and liken social media posts to the utterly personal expressions written in private diaries. This may lead a juror to place significant weight on the social media evidence in their analysis of guilt—and possibly alter the verdict.

While an email or social networking post may be a probative piece of evidence, jurors must have sufficient evidence in order to return a guilty verdict.\(^{42}\) It is the natural course of juror deliberations to place more weight on some pieces of evidence over others and assign varying levels of credibility to witnesses; this does not warrant exclusion of email and SNS evidence. In fact, jurors with knowledge of email and social networking sites are in the best position to judge the credibility of the evidence because they are more aware of potential misuse and other functional problems than someone who has never accessed the websites. Because of this awareness, it is more likely that jurors will view this type of evidence with skepticism and as a piece of the whole, rather than as the proverbial "smoking gun."\(^{43}\) Moreover, a typical judge's instruction will direct jurors

---

38 See Fed. R. Evid. 403 ("The court may exclude relevant evidence if its probative value is substantially outweighed by a danger of . . . unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence.").

39 See Jeffery Bellin, Facebook, Twitter, and the Uncertain Future of Present Sense Impressions, 160 U. PA. L. REV. 331, 362–63 (2012) (contrasting face to face interaction with anonymous social media posts and noting that such normalcy "renders the resulting observations—whether accurate or not—significantly more potent as evidence").

40 Id. at 363 n.116.

41 Leonard M. Niehoff, Of Tweets and Trials, COMMC’NS LAW., Sept. 2010, at 10, 12.

42 See State v. Salinas, 829 P.2d 1068, 1074 (Wash. 1992) (en banc) ("The test for determining the sufficiency of the evidence is whether, after viewing the evidence in the light most favorable to the State, any rational trier of fact could have found guilt beyond a reasonable doubt."); Richmond & D.R. Co. v. Trammel, 53 Fed. 196, 201 (D. Ga. 1892) ("[S]ufficient evidence, ‘is intended that amount of proof which ordinarily satisfies an unprejudiced mind beyond reasonable doubt.’").

43 John Browning argues that social media can provide "smoking gun" revelations. John G. Browning, Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites, 14 SMU SCI. & TECH. L. REV. 465, 470 (2011). However, the example he uses is from an episode of CBS's The Good Wife, where the judge rules in favor of the defendant because of a photo on the plaintiff's Facebook site. Id. While Facebook has certainly made it easier for lawyers to obtain
on how to weigh evidence, how to decide what evidence to believe, and what burden of proof the plaintiff or prosecution must meet. The so-called “faux intimacy” of the Internet should not, on its own, exclude email and SNS evidence.

C. The Hearsay Hurdle

Rule 801(c) defines hearsay as a statement that “the declarant does not make while testifying at the current trial or hearing; and a party offers in evidence to prove the truth of the matter asserted in the statement.” The purpose behind the hearsay doctrine is to preclude information subject to human error.

Statements made in emails and on SNSs, by someone other than the declarant testifying at trial, are considered hearsay if offered for the truth of the matter asserted because they are made outside of the courtroom, and thus the translation of what was actually said is subject to human error.

The current Rules are exhaustive in terms of hearsay exceptions. Case law demonstrates how email messages and social networking posts can be admissions by a party opponent, which the Rules do not consider hearsay, or can fall within the scope of certain hearsay exceptions—namely as a present sense impression; a then existing mental, emotional, or physical condition; and in rare cases, as a business record.

1. Admissions by a Party Opponent

Courts have broadly applied Rule 801(d)(2) to email and social photographs of the opposing party, that is not what opponents of social evidence are concerned about and there is already a Rule providing for their authentication. Proponents of photographs do not need to identify the original photographer as opposed to proponents of email and social media evidence who must do so for the evidence to be relevant. See FED. R. EVID. 1001(c), 1002, 1003 (providing that an original or duplicate photograph is admissible once a proper foundation is laid). Furthermore, pictures do not require the same interpretation that is necessary for the text of emails and social media posts.

See Laurie L. Baughman, Friend Request or Foe? Confirming the Misuse of Internet and Social Networking Sites by Domestic Violence Perpetrators, 19 WIDENER L.J. 933, 949-50 (“[W]hen trying to admit the records of Internet service providers and social networking sites, that information also could be considered hearsay because the data is subject to human error—the driving purpose behind the hearsay doctrine.”).

FED. R. EVID. 801(c).

See id.

See Monotype Corp. PLC v. Int’l Typeface Corp., 43 F.3d 443, 450 (9th Cir. 1994) (“Email is far less of a systematic business activity. [It] is an ongoing electronic message and retrieval system.”); New York v. Microsoft Corp., No. CIV A. 98-1233(CKK), 2002 WL 649951, at *2 (D.D.C. Apr. 12, 2002) (stating that absent evidence that a company’s “regular practice” is to write and maintain emails, such emails are not “sufficiently trustworthy” for the business record exception); United States v. Ferber, 966 F. Supp. 90, 99 (D. Mass 1997) (holding that there must be a routine business duty to maintain emails in order to qualify for the business record exception).

FED. R. EVID. 801(d)(2) (providing that the following types of statements offered against an opposing party are not hearsay: (1) one “that was made by the party in an individual or representative
networking evidence. In *Vermont Electrical Power Co. v. Hartford Steam Boiler Inspection and Insurance Co.*, the defendant successfully argued that “intra-company correspondence,” which articulated how certain damage occurred, was an admission by a party opponent and was therefore admissible as non-hearsay.\(^4\) Several courts followed the logic expressed in *Vermont Electrical Power Co.* and have admitted a party’s website and emails into evidence under Rule 801(d)(2).\(^5\) For example, the District of Oregon admitted representations made by a defendant on his website.\(^6\) The court accepted the plaintiff’s testimony regarding what he viewed on the website in furtherance of their decision.\(^7\) The Northern District of Illinois also adopted the District of Oregon’s reasoning in admitting website printouts as non-hearsay, partially because they were verified by the Internet Archive Company that retrieved the copies.\(^8\)

The standards for admitting email content as non-hearsay can also apply to SNS posts. Information posted by a party opponent can be used as an admission.\(^9\) One attorney tried to argue, as a defense strategy, that the victim’s bruises did not come from his client but rather from falling down while intoxicated, since the victim wrote about drinking and having a “pretty rough night” on her Facebook page.\(^10\) The court rejected the evidence on relevancy grounds, noting time frame issues, and that it


\(^5\) See, e.g., Price v. Fox Entm’t Grp., Inc., No. 05 Civ.5259 SAS, 2007 WL 241386, at *2 (S.D.N.Y. Jan. 26, 2007) ("[T]he statement contained in the email that ‘Rawson Thurber would like to meet with you’ implicitly conveys a statement by Thurber, and as such, is not hearsay under FRE 801(d)(2)"); Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 454 F. Supp. 2d 966, 973 (C.D. Cal. 2006) (admitting emails under 801(d)(2) where the proffering party laid a foundation to show that "an otherwise excludable statement relates to a matter within the scope of the agent’s employment"); United States v. Safavian, 435 F. Supp. 2d 36, 43 (D.D.C. 2006) (admitting emails as admissions by defendant and also finding that "[t]he context and content of certain e-mails demonstrate clearly that [the defendant] ‘manifested an adoption or belief in the truth of the statements of other people’ so as to be admissible under Fed. R. Evid. 801(d)(2)(B)). The holding in *Grokster* was later adopted in *Avondale Mills, Inc. v. Norfolk Southern Corp.*, C/A No. 1:05-2817-MBS, 2008 WL 6953956, at *5 (D.S.C. Feb. 21, 2008) (denying a motion in limine to exclude emails).


\(^7\) Id.

\(^8\) See Telewizja Polska USA, Inc. v. Echostar Satellite Corp., No. 02 C 3293, 2004 WL 2367740, at *6 (N.D. Ill. Oct. 15, 2004) ("Federal Rule of Evidence 901 ‘requires only a prima facie showing of genuineness and leaves it to the jury to decide the true authenticity and probative value of the evidence.’"). The court went on to state that “the Internet Archive does not fit neatly into any of the non-exhaustive examples listed in Rule 901” because it “is a relatively new source for archiving websites.” Id. However, the plaintiff failed to present any evidence that the Internet Archive was unreliable, and, as the court noted, was “free to raise its concerns regarding reliability with the jury.” Id.

\(^9\) Baughman, *supra* note 45, at 950–51.

violated rape shield laws by referencing "instances of what could be termed misconduct on the part of the Victim." The court seemed to imply, however, that, absent relevancy issues, the evidence could be used as an admission by a party opponent and as a means to impeach a witness.

Consequently, forwarding an email could be considered a tacit admission, meaning that a person acquiesces to a statement through an act or silence. In Sea-Land Services, Inc. v. Lozen International, LLC, the Ninth Circuit held that a forwarded email with statements from an employee supporting the email's content could be admitted as an adoptive admission, which is expressly defined as not hearsay. Additionally, Facebook allows users to endorse posted content by affirmatively "liking" the post. An attorney could potentially argue that such approval of a friend's post qualifies as an adoptive admission.

2. "A Specialized Present Sense Impression Application"

According to the Advisory Committee that drafted the Federal Rules of Evidence, allowing tweets and social media posts under Rule 803(3) is "essentially a specialized application" of the present sense impression exception. Rule 803(3) exempts from the hearsay rule, "[a] statement of the declarant’s then existing state of mind (such as motive, intent, or plan) or emotional, sensory, or physical condition (such as mental feeling, pain, or bodily health) . . . ." There are few cases where courts have applied Rule 803(3), because, as the Advisory Committee notes, "excluding statements of memory or belief is 'necessary to avoid the virtual destruction of the hearsay rule.'" However, the fact that these statements are written prevents the translation errors that the hearsay rule exists to prevent.

---

56 Id. at 579.
57 Id.
58 See Fed. R. Evid. 801(d)(2)(B) (defining a statement as non-hearsay if it is offered against an opposing party and "is one the party manifested that it adopted or believed to be true").
59 285 F.3d 808, 821 (9th Cir. 2002); see also In re Oil Rig "Deepwater Horizon," MDL No. 2179, 2012 WL 85447, at *4 (E.D. La. Jan. 11, 2012) ("The PSC argues that many of the emails that were forwarded by employees of the parties are adoptive admissions. This is a plausible argument under Rule 801(d)(2)(B), which makes admissible statements of which a party manifested its adoption or belief."); Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, 454 F. Supp. 2d 966, 973 (C.D. Cal. 2006) ("If content created by individuals other than the creator of an email is incorporated into the email, the incorporated content is also admissible non-hearsay under Rule 801(d)(2)(B).").
60 This argument may be difficult to make, however, as the court in Oil Rig "Deepwater Horizon" noted that a "forwarded email is only an adoptive admission if it is clear that the forwarder adopted the content or believed in the truth of the content." 2012 WL 85447, at *4; see also Baughman, supra note 45, at 951 (noting that clients must pay close attention to what they post on social networking sites given this "seemingly unfettered ability to introduce potentially damaging evidence").
62 Fed. R. Evid. 803(3).
63 Brenner, supra note 61, at 17.
avoid.

The comprehensive specialized application of this exception is appropriate for email and SNS evidence, because, as previously noted, the "faux intimacy" of email and SNSs leads to "candid, perhaps too-candid, statements of the declarant’s state of mind, feelings, emotions, and motives." Additionally, other hearsay exceptions, such as present sense impression and excited utterances, are very difficult to apply to SNS posts and emails given that these exceptions require that the writer did not have time to reflect or fabricate. Nonetheless, one court did, in fact, apply this standard to admit emails detailing a co-conspirator’s plan, intent, and motive.

3. Past Recollection Recorded

Emails and SNS data can also aid attorneys with witnesses who once had relevant personal knowledge about a matter, but who now have an insufficient recollection to testify at trial. Attorneys can qualify email or SNS evidence that is shown to have been “made or adopted by the witness when the matter was fresh in the witness’s memory” as a past recorded recollection. While the information may not be received as an exhibit unless offered by an adverse party, blogs, posts, and emails can serve as a “memorandum or record” to a witness who cannot remember a once-perceived incident. Allowing attorneys to use witnesses’ blogs is particularly crucial given their prevalence, and the rate at which they have replaced personal journals.

D. Best Evidence Rule

A final potential barrier, the best evidence rule, may present an
evidentiary problem for attorneys seeking to admit emails and SNS evidence. The rule states that "[a]n original writing, recording, or photograph is required in order to prove its content." Production of a true original of an email or social networking page is not necessarily possible because both are always electronic. However, the definition of "original" includes "any printout or other output readable by sight, shown to reflect the data accurately." As such, it seems likely that a printout would suffice.

IV. THE MYRIAD WAYS TO PROVE ATTRIBUTION UNDER THE CURRENT RULES

The aforementioned case law suggests that authentication of the evidence is the most important factor in a court’s hearsay and relevancy analysis. The fact that the text of emails and websites look like admissions, however, is insufficient without some proof of attribution. Certain statements are only relevant to the case if the proponent of the evidence can offer the context in which they were spoken, and demonstrate by whom they were spoken.

Rule 901(a) requires the “authentication or identification as a condition precedent to admissibility.” If an attorney is unable to lay a proper foundation for attribution, the court must exclude the evidence. “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.”

Authenticating electronic information is a two-step process. First, the offeror must lay a satisfactory foundation for the jury to find that the evidence is what the proponent claims. Second, since “authentication is essentially a question of conditional relevancy, the finder of fact ultimately resolves whether evidence admitted for its consideration is that which the proponent claims.” Evidence falls into two categories for purposes of

70 Fed. R. Evid. 1002.
71 Baughman, supra note 45, at 953.
72 Id. (quoting Fed. R. Evid. 1001(3) and Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d, 1146, 1155 n.4 (C.D. Cal. 2002)) (internal citations omitted).
73 Bruther v. Gen. Elec. Co., 818 F. Supp. 1238, 1240 (S.D. Ind. 1993) (citing Fed. R. Evid. 901(a)) (articulating that the “rationale behind this Rule is that absent a showing that the evidence is what the proponent alleges, it has no relevance”).
74 Fed. R. Evid. 901(a). Courts have noted that evidence necessary to support this standard is often lower than the preponderance of the evidence standard in civil cases. See State v. Bell, 882 N.E.2d 502, 512 (2008) (citing Burns v. May, 728 N.E.2d 19 (Ohio Ct. App. 1999)) (finding that the standard is whether a reasonable juror could conclude “that the offered printouts are authentic”).
75 Fed. R. Evid. 901(a); Paul W. Grimm & Lisa M. Yurvit, Electronically Stored Information in Maryland and Federal Courts: Discovery, Admissibility, and Ethics 269 (quoting United States v. Branch, 970 F.2d 1368, 1370 (4th Cir. 1992)).
76 Id. (citing Branch, 970 F.2d at 1370).
authentication: evidence that self-authenticates under Rule 902, and evidence that requires authentication by way of illustration under Rule 901(b). Since email and SNSs do not fit into any of the categories outlined in Rule 902 and also lack the "indicia of reliability" of self-authenticating materials, they must be authenticated by way of illustration.

The authentication requirement is the biggest hurdle to the admission of email and SNS evidence at trial because some judges are convinced that the content is "inherently insecure and unreliable." For example, the court in St. Clair v. Johnny's Oyster & Shrimp Inc., found electronic evidence "inherently untrustworthy" based on the view that the Internet is "one large catalyst for rumor, innuendo, and misinformation." The court went on to say that "evidence procured off the Internet is adequate for almost nothing." To take this view of email and SNS evidence demonstrates ignorance of the changing times and a disregard for the unreliability of evidence traditionally admitted at trial. As the Pennsylvania Superior Court noted in In re F.P., "the same uncertainties exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen." Perhaps not surprisingly then, the court found that Internet evidence can be properly authenticated.

There are numerous ways email messages and SNS evidence can be authenticated under the current Rules. The problem is that there are too many methods of authentication, and not all are adopted by each jurisdiction in the same manner, if at all. This leads to confusion over what meets the threshold for authentication of emails and SNS. It also

---

77 See FED. R. EVID. 902 (listing the following twelve documents that self-authenticate: domestic public documents under seal, domestic public documents not under seal, foreign public documents, certified copies of public records, official publications, newspapers and periodicals, trade inscriptions and the like, acknowledged documents, commercial paper and related documents, presumptions under a federal statute, certified domestic records of regularly conducted activity and certified foreign records of regularly conducted activity).

78 Kevin F. Brady et al., The Sedona Conference Commentary on ESI Evidence & Admissibility, 9 SEDONA CONF. J. 217, 220 (2008); accord Chisholm v. Idaho Dept' of Water Res., 125 P.3d 515, 519, 165 (2005) (holding that a hearing officer did not err in excluding an email message as evidence because "email is unreliable"); see also In re F.P., 878 A.2d 91, 95 (Pa. Super. Ct. 2005) ("The argument is that emails or text messages are inherently unreliable because of their relative anonymity . . .").


80 Id. at 775.

81 In re F.P., 878 A.2d at 95.

82 Id.

83 See Katherine Minotti, The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession, 60 S.C. L. REV. 1057, 1061 (2009) (lamenting that "there is no consensus" among the "handful of decisions that address social networking sites").

84 Some courts adopt the standard of sufficient indicia of reliability that show it is "more likely than not" that the evidence is authored by a certain individual. Tele Atlas N.V. v. NAVTEQ Corp., No. C-05-01673, 2008 WL 4809441, at *8 (N.D. Cal. Oct. 28, 2008). Others, however, hold that the
A. The Many Methods of Authentication

Some courts allow authentication by testimony from witnesses who either sent or received the email message or posted the social networking content. The witness must verify that the message is a personal correspondence of his or hers, and must have personal knowledge in order to testify. Someone without knowledge of the transmissions at issue cannot authenticate an email unless the witness has enough technical knowledge of the process to be qualified as an expert witness.

In People v. Clevenstine, the Appellate Division of the New York Supreme Court affirmed the trial court’s decision to admit instant messages from MySpace because both victims testified that they instant messaged the defendant about the sexual activities in question. Additionally, an investigator from the State Police’s computer crime unit testified that he retrieved the conversations from the victims’ hard drives, and one of MySpace’s legal compliance officers stated that the messages were exchanged through accounts owned by the victims and the defendant.

The court noted that “‘[a]uthenticity is established by proof that the offered evidence is genuine and that there has been no tampering with it.’” The defendant did, in fact, argue that it was possible for someone to tamper with his account, but the court stated that “the likelihood of such a scenario
presented a factual issue for the jury." 93

For authentication purposes, "[c]ourts generally fall into three camps with respect to the scope of testimony that 901(b)(1) requires." 94 Some courts employ a standard similar to authenticating a letter, and require testimony, in the form of a statement or an affidavit, from the website's web master or from someone else with personal knowledge "that the information was posted by the individual." 95 Other courts are much more lenient and apply the same standard used for photographs; the person who created the screenshot must testify that it "accurately reflects the content of the Web site and the image of the page on the computer at which the [screen shot] was made." 96 While the photography method may be acceptable for generic websites, it is insufficient for SNS evidence. The accuracy of the screen shot is certainly important, but the central question is attribution, and this "camp" of testimony does not, on its own, verify authorship. 97

The last group of courts conduct a more fact intensive inquiry. These courts require proponents to meet a prima facie burden regarding "incentive and ability to falsify evidence." 98 Of the three approaches, the third is most appropriate; it is specifically tailored to email and SNS evidence and aptly addresses concerns over hacking and tampering with the websites. The virtual records exception proposed in Part V adopts a similar standard in an effort to limit some of the variances demonstrated by these three camps.

Some courts, however, do not necessarily admit email or SNS evidence even when a witness with personal knowledge provides testimony regarding their authenticity. For example, the Court of Appeals of Kentucky stated that a trial court did not abuse its discretion in excluding emails from evidence, even though the victim in the case testified that she received the emails and the defendant acknowledged to

93 Id. at 1451. Defendant suggested that tampering took place in the form of another accessing his MySpace account and sending messages under his username. Id.
94 M. Anderson Berry & David Kiernan, Authenticating Web Pages as Evidence, LAW TECH. NEWS, Jan. 21, 2010.
95 Id. (citing In re Homestore, Inc. Sec. Litig., 347 F. Supp. 2d 769, 782–83 (C.D. Cal. 2004); Wady v. Provident Life & Accident Ins. Co. of Am., 216 F. Supp. 2d 1060, 1064 (C.D. Cal. 2002)).
97 See id. ("Notably, courts in the second camp do not appear to require the proponent to authenticate the information as authored or sponsored by the individual to whom it is attributed. Instead, the party need only show that the screen shot reflects what was on the site. Presumably, the issue of authorship or sponsorship will be the subject of cross-examination and further proof.").
98 Id. (citing United States v. Jackson, 208 F.3d 633, 637 (7th Cir. 2000)). The Court excluded screen shots because the proponent could not prove that the "information was actually put on the website by the site's sponsor." Id.
the victim that she was the sender. If testimony is insufficient, or if a witness with personal knowledge is unavailable, some courts have turned to circumstantial indicia of reliability including the typical format of a printed email, indicating the sender, recipient, date and subject line; a reference to the nickname of the author in the body of the email; a recipient’s familiarity with the email address due to a chain of communication; or a conversation between the recipient witness and the sender about the contents of the message. A sub-form of authentication through circumstantial indicia is the use of an exemplar; parties can validate messages through comparison to a previously authenticated specimen. For instance, if an email address is ambiguous and cannot readily be used to identify the sender, it can be compared with an authenticated exhibit containing distinctive characteristics to connect the sender to that email address.

Circumstantial evidence is also frequently used to authenticate the contents of a website. Indicia such as the appearance of the screenshot, download dates, and web addresses can lead a reasonable juror to believe that the website printout is what the proponent claims. For example, the Central District of California ruled that when a party offers the content of its own website into evidence there is a “circumstantial indicia of authenticity.”

While this method of authentication seems self-serving, courts often distinguish between information generated from a party’s website and information generated from a non-party’s website, generally finding the former to be more authentic. For example, the court in Florida Conference Ass’n of Seventh-Day Adventists v. Kyriakides admitted to the Security Exchange Commission reports posted by the defendant on the Internet. The court rejected the defendant’s argument that the reports should be barred under Jackson and St. Clair because in those cases the

---

100 Joseph, supra note 86, at 14-15.
101 Fed. R. Evid. 901(b)(3).
105 Id. ("[T]he Court finds that, as a general rule, the [owner’s] declaration is sufficient to establish the exhibits’ authenticity.").
website postings were made by non-parties. Facebook deems each individual user to be the owner of all posted content; each user owns and manages the content on their personal webpage, despite the fact that it is stored on Facebook's system. Therefore, according to the Florida Conference court, a party's offer of its own social networking page into evidence carries circumstantial indicia of authenticity. While circumstantial evidence is clearly useful, courts have not specified which indicia they generally consider to be more or less reliable.

Technical experts have also been used to verify Internet evidence, particularly when there is ambiguity or someone denies sending a message. Internet Service Providers ("ISP") assign every computer a thirty-two-bit numeric Internet Protocol ("IP") address. "The IP address serves as an identifier for the computer on the internet." If someone regularly uses the same computer, the IP address could be used to link that individual to the computer. Some courts have found that IP addresses make emails easier to trace than written letters. However, IP addresses may not prove useful without testimony or other evidence to place the sender or poster at that specific address, unless, of course, the address turns out to be the party's residence or place of work. It is important to remember that email and SNSs may also be accessed from any computer and at any time.

B. Problems with Self-Authentication

As previously mentioned, email and SNSs lack the "indicia of reliability" for inclusion into the several documents that the Rules accept as self authenticating. Rule 902 recognizes instances where extrinsic evidence is not necessary in order for the evidence to be admitted. One federal district court has determined that email addresses are self-authenticating. The Northern District of Illinois granted a motion in limine.

---

108 Id. at 1226.
109 See Statement of Rights and Responsibilities, FACEBOOK, http://www.facebook.com/terms.php (last visited May 16, 2012) [hereinafter Statement of Rights] ("You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings.").
111 Id.
112 Id.
113 See, e.g., Clement v. Cal. Dept' of Corr., 220 F. Supp. 2d 1098, 1111 (N.D. Cal. 2002) ("The evidence in the record suggests that Internet-produced materials are, in fact, easier to trace than anonymous letters because the major email providers include a coded Internet Protocol address . . . in the header of every email.").
114 FED. R. EVID. 902.
to admit statements contained in two email messages under Rule 902(7). According to the court’s decision, if the email address contains the name of a business or organization (usually in an abbreviated form following the @ symbol) it can be self-authenticating under Rule 902(7), which provides for “trade inscriptions and the like.” Under the court’s analysis, it follows that if the email address displays the name of the sender along with a company name (i.e. employee@business.org), it is a trade inscription of the employee.

The Illinois court’s reasoning is flawed, however, as it does not address the concerns from opponents of Internet evidence. According to the court’s opinion, a website screenshot is self-authenticating simply because the company logo appears somewhere on the page. While it is much easier to create a false webpage than it is to access a company’s email account, the court still applied Rule 902(7) much too broadly. The rule is traditionally used to indicate ownership of widely known products, such as vehicles, cattle brands, and food items—in other words, products whose brandings are not likely forged. On the other hand, it is much easier for someone to write on another person’s letterhead or access another individual’s personal email account. The possibility of forgery warrants a somewhat higher burden of proof for this type of evidence than that which courts have applied under Rule 902.

116 Id.; see also FED. R. EVID. 902(7) (providing that extrinsic evidence of “inscription[s], sign[s], tag[s], or label[s] purporting to have been affixed in the course of business and indicating origin, ownership, or control” is not required for authentication).
118 See id. at 243 (“To illustrate the potential implications of the argument that an email address is sufficient to authenticate the entire e-mail message, if a trade inscription automatically authenticated a document bearing the trade inscription, then all documents appearing on corporate letterhead would be self-authenticating.”).
119 See State v. Eleck, 23 A.3d 818, 821 n.4 (Conn. App. 2011) (“Typically, electronic messages do have self-identifying features. For example, e-mail messages are marked with the sender’s e-mail address, text messages are marked with the sender’s cell phone number, and Facebook messages are marked with a user name and profile picture. Nonetheless, given that such messages could be generated by a third party under the guise of the named sender, opinions from other jurisdictions have not equated evidence of these account user names or numbers with self-authentication. Rather, user names have been treated as circumstantial evidence of authenticity that may be considered in conjunction with other circumstantial evidence.”); Robins, supra note 117, at 240, 242 (explaining that the rule of self authentication for trademarks “is justified by the serious penalties that the trademark laws apply to one who uses the mark of another without authorization” and further arguing that actions that simply violate company policies do not have the “same indicia of trustworthiness”).
V. THE ADVISORY COMMITTEE SHOULD ADD A “VIRTUAL RECORDS” EXCEPTION TO THE FEDERAL RULES OF EVIDENCE

Rule 901(b)(7) allows authentication by “public records.” Public records “are regularly authenticated by proof of custody, without more.” To apply Rule 901(b)(7), a person must show that the office holding the record is the legal custodian of the record. Custody may be proven through testimony of an officer able to validate the custodianship, or through testimony of a witness with knowledge that the record is from a specific office. The types of public records that the Rule encompasses include judicial records, tax returns, military records, and data compilations, which may include those stored in computers.

Essentially, Rule 901(b)(7) allows authentication for documents that carry some indicia of reliability. However, courts have held that the offeror of a public record does not need to demonstrate that the computer system keeping the public record is reliable or accurate. In United States v. Meienberg, the government submitted computer printouts reflecting approval numbers assigned to the defendant’s firearm business. Despite the defendant’s concerns over the accuracy of the computer program, the Tenth Circuit ruled that a witness’s testimony was enough to authenticate the document. The court further noted that, according to Rule 901(a), all that a proponent must do is “present evidence sufficient to support a finding that the matter in question is what its proponent claims.”

Emails and SNS posts, along with letters and personal checkbooks, are considered private records because each individual user acts as the legal custodian of the written and uploaded content. But the simple fact that they are private papers does not make them more or less reliable than public records, and it is possible to present evidence that the emails and posts are what the proponent claims. For example, it seems that checkbooks have become almost obsolete; many people simply rely on

120 See FED. R. EVID. 901(b)(7) (“Evidence that: (A) a document was recorded or filed in a public office as authorized by law; or (B) a purport public record or statement is from the office where items of this kind are kept . . . .”).
121 See Romano, supra note 106, at 1754 (quoting the Advisory Committee).
123 Id.; Romano, supra note 106, at 1755 (citing FED. R. EVID. 907(b)).
124 Lorraine, 241 F.R.D. at 548.
125 See Romano, supra note 106, at 1754 (citing United States v. Meienberg, 263 F.3d 1177, 1181 (10th Cir. 2001)). Meienberg held that “[a]ny question as to the accuracy of the printouts, whether resulting from incorrect data entry or the operation of the computer program, as with inaccuracies in any other type of business records, would have affected only the weight of the printouts, not their admissibility.” 263 F.3d at 1181 (citations omitted) (internal quotations omitted).
126 Id.
127 Id. (internal quotations omitted).
128 See Statement of Rights, supra note 109 (“You own all of the content and information you post on Facebook . . . .”).
their bank's online software to monitor their spending and balance their account. Certainly information maintained on a single database is more reliable than a lay individual's own accounting and filing system. And, realistically, data compilations stored in a computer are just as vulnerable to spoliation as one's Facebook or MySpace page. The Rules give more credit to tax returns stored in a public office, which are accessible to any staff member, than to SNS posts made by only those with access to an individual's account. Facebook can thus be likened to a private record keeping office, as each post is backed up on the system and remains there even after deletion.129

A. Proposed Virtual Records Rule 901(b)(11)

In State v. Eleck, a case of first impression for the Connecticut Appellate Court regarding SNS evidence, the court conceded that “evidence that tends to authenticate a communication is somewhat unique to each medium.”130 Authenticating SNSs and emails is inherently different than authenticating telephone calls and writings because the same identifiers are not present.131 As such, the Advisory Committee should create a new rule.132 A virtual records exception would act similarly to the public records exception found in Rule 901(b)(7). The exception would be applicable to only those documents created by individuals for a private purpose and exist solely in electronic format on a password-protected database. The Rule should read as follows:

Virtual records. Evidence that private pass code protected papers including, but not limited to, messages from personal email accounts, online journals, pages from social networking websites, and online bank records, are (A) authored by the account holder; (B) in a condition as to

---

129 See id. ("When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time . . . .").

130 State v. Eleck, 23 A.3d 818, 823 (Conn. App. Ct. 2011) (noting that the Connecticut Supreme Court has held that “[a] sufficient foundation is laid when the subject matter of the conversation, evidence of its occurrence, and prior and subsequent conduct of the parties fairly establish the identity of the person with whom conversation occurred” and that “the authorship of letters on a computer hard drive could be authenticated by the mode of expression of the writing, detailed references to the defendant’s finances and circumstantial evidence linking the defendant’s presence at home with the time the letters were created on his home computer”).

131 See Minotti, supra note 83, at 1067–68 (stating that “[a]uthentication of Internet postings is unique” and a “fact-intensive inquiry”).

132 While the Connecticut Appellate Court did not expressly endorse the adoption of a new rule, the court did note that it might be useful “to investigate the appropriateness of new rules specifically pertaining to electronic evidence.” Eleck, 23 A.3d at 823 n.8.
leave no reasonable suspicion concerning authenticity; and
(C) exist solely on a reliable Internet database.\textsuperscript{133}

To comply with proposed Rule 901(b)(11), proponents of such evidence
should be required to provide corroboration, submit to an internal
balancing test performed by the judge, and request a special jury
instruction.

1. Corroboration

Proposed Rule 901(b)(11) would adopt a form of the corroboration
rule that is applied to the admission of an accused’s confession in a
criminal trial.\textsuperscript{134} Recognizing that statements from the perpetrator of a
crime or tort can carry heavy weight, courts should require additional
evidence to test the statements’ authenticity. While the corroboration rule
in American jurisprudence takes several forms, it protects the accused from
undue prejudice.\textsuperscript{135}

Essentially, the proponent of email or SNS evidence should be
required to remove any reasonable suspicion of legal custodianship by
offering evidence of access. To do so, the offerors could use any
combination of the following evidence, as established by the case law
above: (1) testimony of the account holder or a witness who saw the user
write or upload the content; (2) evidence that the alleged author regularly
uses a specific username or email address; (3) proof that the content of the
message contains information that the alleged author is likely to have
knowledge of or that the tone and tenor of the evidence is that normally
used by the alleged author; (4) references to nicknames or other personal
information in the content of the email or post; (5) chain of
communication; and (6) usage history.

While an IP address or access to a specific computer may be helpful, it
is important to keep in mind that email and SNS evidence does not just

\textsuperscript{133} Reliable Internet databases include those whose parent company maintains a business office,
or that has a website master. For example, a bank’s online accounting of one’s finances is likely to be
more reliable than one’s own checkbook. These websites have automated databases that track each
time that a person logs onto the website and performs other actions (e.g., debiting their account, paying
a bill). These websites are also less likely to misplace important documents or make accounting errors.
As previously mentioned, Facebook and MySpace both have offices that keep and maintain records
pertaining to users’ profiles.

\textsuperscript{134} Russell L. Miller, \textit{Wrestling with MRE 304(g): The Struggle to Apply the Corroboration Rule},
178 MIL. L. REV. 1, 4 (2003) ("There are several species of the corroboration rule in American
jurisprudence, and all require evidence in addition to the confession as a test of reliability.").

\textsuperscript{135} See Sandra Guerra Thompson, \textit{Beyond a Reasonable Doubt? Reconsidering Uncorroborated
emerged during the late nineteenth century as a means of protecting men from an ‘untruthful, dishonest,
or vicious complainant.’ The traditional view was that the rule would ‘minimize the risk that false
charges will be brought; that it balances the sympathy for the victim felt by the jury . . . ‘").
exist on a single computer. Instead, the content exists on a virtual database
that one may access from any computer. In this regard, the proponent
could prove access by providing a court with the names of individuals who
had access to the account at the time the content was sent or uploaded.
Whether others with access to the account had a motive to tamper with the
account should be a question for the trier of fact.

An additional method of corroboration would be a computer search.
As the Maryland Court of Appeals suggested, an examination of a
computer's Internet history and hard drive may help to determine whether
the computer was utilized to create the social networking profile or email
account. The court went on to quote the statement of the Deputy
General Counsel of Stroz Friedberg, LLC: "Since a user unwittingly leaves
an evidentiary trail on her computer simply by using it, her computer will
provide evidence of her web usage." Because SNSs and email accounts
can be accessed on any Internet-capable computer, an attorney would need
to conduct additional discovery to determine how many computers the
poster was able to access at the time of usage.

Opponents of social media and email evidence cannot ignore the fact
that circumstantial evidence is often enough for courts and juries to decide
a matter, even one as serious as murder. Courts should not hold SNS
and email evidence to a higher standard than other similar evidence, such
as confessions, which are routinely admitted into court as long as they are
corroborated. If the proponent can offer sufficient corroboration, he or she
should be able to benefit from the evidence.

137 Id. (citation and quotations omitted).
138 See Holland v. United States, 348 U.S. 121, 140 (1954) ("Circumstantial evidence in this
respect is intrinsically no different from testimonial evidence."); United States v. Martinez, 54 F.3d
1040, 1043 (2d Cir. 1995) (concluding "the jury's verdict may be based entirely on circumstantial
evidence" and that "it is the task of the jury, not the court, to choose among competing inferences")
(internal citations omitted); Adams v. Aiken, 41 F.3d 175, 181 (4th Cir. 1994) ("Circumstantial
evidence is good evidence provided it meets the tests laid down by the law."); United States v. Wigoda,
521 F.2d 1221, 1225 (7th Cir. 1975) (stating that "[a]ll that is necessary [of circumstantial evidence] is
that it can convince a jury beyond a reasonable doubt of the defendant's guilt") (internal citations
omitted); United States v. Shahane, 517 F.2d 1173, 1177 (8th Cir. 1975) ("Circumstantial evidence
does not differ in principle from direct evidence, and that in order for a jury to convict on
circumstantial evidence it is not necessary that the evidence exclude every reasonable hypothesis
except that of guilt but simply that it be sufficient to convince the jury beyond a reasonable doubt that
the defendant is guilty."); United States v. Young, 291 F.2d 389, 390 (6th Cir. 1961) ("Circumstantial
evidence, if strong enough to convince a jury of defendant's guilt beyond a reasonable doubt, is
sufficient to take a case to the jury and sustain a verdict. It is not necessary that it be such evidence as
would remove every reasonable hypothesis except that of guilt.") (internal citations omitted).
139 See United States v. Rounds, 30 M.J. 76, 80 (C.M.A. 1990) (finding that proof of access and
opportunity is "enough" corroboration).
2. Internal Balancing Test

Pursuant to Rule 403, a judge presiding over a case where email or SNS evidence is offered would need to conduct a standard balancing test. First the judge must assess the probative value of the evidence. In doing so, the judge must take into account how much of the corroboration described in the previous section the attorney can provide for the evidence's authentication. The analysis would not depend solely on the amount of corroboration, but rather on the reliability of corroboration. A single computer search may prove more trustworthy than the testimony of several witnesses. Second, the judge must analyze the prejudicial effect of the evidence, taking into account authenticity issues. In the event that the judge determines that suspicions regarding authenticity outweigh the probative value, the evidence would be excluded.

3. Jury Instruction

As a final safeguard, a judge must give a special instruction to a jury charged with considering email and SNS evidence. While the judge would have already performed the standard balancing test, the jury would provide a second review as to whether the corroboration was sufficient. In criminal cases, the judge would alert jurors to use great caution in weighing the testimony of corroborating witnesses and inform them that they may not give weight to any evidence that they do not believe to be sufficiently authenticated—meaning that there is no reasonable suspicion that there is a connection between the email or SNS content and the author. In civil cases, the judge would alert jurors to exercise caution in weighing the corroborative evidence and that, in evaluating the email and SNS evidence along with the corroborative evidence, they must find a sufficient link between the evidence and the litigant in order to consider the evidence in their analysis.

VI. IMPLICATIONS OF USING EMAIL AND SOCIAL NETWORKING EVIDENCE IN THE LEGAL PROFESSION

The use of email and SNS evidence presents both good and bad implications for our legal system. On one hand, attorneys have access to a wealth of knowledge and information about their clients and opponents that previously were not readily accessible. On the other hand, such evidence inadvertently may make all individuals more accessible to the

140 Thomas J. Reed, Evidentiary Failures: A Structural Theory of Evidence Applied to Hearsay Issues, 18 AM. J. TRIAL ADVOC. 353, 367 (1994); see also State v. Eleck, 23 A.3d 818, 824 (Conn. App. Ct. 2011) (holding that the content of the exchange did not provide “distinctive evidence of the interpersonal conflict” between the defendant and another).
141 Reed, supra note 140, at 367.
legal system, increase the workload for attorneys and judges, and foster uncertainty in jurors' minds—potentially leading to unfair verdicts.

Email and SNS evidence can aid prosecutors in implicating dangerous individuals and holding them responsible for their crimes. For example, a prosecutor in California used Facebook to find a man that was charged with domestic violence by obtaining the suspect's friend list in order to gather names of relatives and employers, and then mailing letters to the suspect in their care.\textsuperscript{142} SNSs have also been useful in prosecuting gang related crime, leading to safer communities.\textsuperscript{143} A deputy county attorney in Arizona noted that while gang members do not openly admit to their crimes on SNSs, they talk about "behavior and antics" that relate to law enforcers' suspicions.\textsuperscript{144} Conversely, the content can be a defense tool; a solo practitioner in Ohio was able to prove that his client was not the initial aggressor by a video on the other suspect's MySpace page.\textsuperscript{145} The court in \textit{State v. Gaskins}, allowed the defendant charged with statutory rape, to admit pictures from the victim's MySpace page in order to show that she looked much older than she actually was at the time.\textsuperscript{146} These cases demonstrate that email and SNS evidence has not given prosecutors an advantage over defense attorneys.

SNS evidence has proved useful not only in criminal proceedings, but in civil litigation as well. Divorce lawyers have found a wealth of information about an opposing party through Facebook, MySpace, and other social networking pages. For example, attorneys have encountered evidence of a father stating that he did not have children on his online dating profile, while he was, in fact, seeking primary custody of his child.\textsuperscript{147} In another case, attorneys found pictures of the opposing party smoking marijuana and evidence that a mother was playing Facebook games instead of attending her child's events.\textsuperscript{148} Facebook also played a large role in the $4.2 million verdict awarded to the family of Jack Phoummarath, a University of Texas student who died of alcohol poisoning.

\textsuperscript{142} Larry Altman, \textit{Prosecutors Track Domestic Violence Suspect Using Facebook}, \textit{Daily Breeze}, June 29, 2011, at 3A.
\textsuperscript{143} Edward M. Marsico, Jr., \textit{Social Networking Websites: Are MySpace and Facebook the Fingerprint of the Twenty-First Century?}, 19 Widener L.J. 967, 968 (2010) (noting that “[r]ecent police officers routinely use social networking sites to investigate crimes” and that “criminals are among the first to utilize technology for devious purposes”); Minotti, supra note 83, at 1060.
\textsuperscript{145} Id.
\textsuperscript{146} Id.
poisoning during his fraternity’s initiation party. The Phoummarath’s attorney used photographs both to identify fraternity members, and to discredit fraternity members’ testimony. The case skyrocketed from twenty to ninety-nine named defendants through the use of SNS evidence.

In addition to parties, attorneys are using SNS to investigate witnesses as well. Some are wary that content on potential experts or witnesses’ accounts may affect their credibility. While some attorneys consider this type of due diligence an advantage over their opponent, others believe “they may now just be keeping up.” The implication is that failure to research parties’ social media is negligence at best. As demonstrated by the previously mentioned cases, Facebook and MySpace have a prominent place in legal research and trial advocacy.

MySpace and Facebook both describe themselves as services for friends, family, and co-workers to communicate and stay connected. But, as more individuals choose to create online profiles, “they may be inadvertently making themselves more accessible to the legal system.” While this is an advantage for the legal profession, it is a great concern for the public. Self-incrimination and privacy issues have arisen from the use of email and SNSs in the workforce and education system. And, when they do, lawyers will need to be prepared to defend the evidence, as any instruction to delete SNS evidence will be considered spoliation, and can result in severe penalties.

149 Justin Rebello, Using Social Networks to Investigate Your Case, LAWYERS USA, Aug. 11, 2008, at 21.
150 Id.
151 Id.
152 Stevenson, supra note 146 (“Janice V. Mitrius . . . says she regularly checks [MySpace and Facebook] when conducting due diligence on potential experts or opposing counsel: ‘I’m primarily looking for information that may affect credibility, and it’s always interesting to see if they’ve put something on one of these sites.’”).
153 Id.
154 See About, FACEBOOK, https://www.facebook.com/facebook/info (last visited Apr. 8, 2012) (“Facebook’s mission is to give people the power to share and make the world more open and connected.”); Myspace.com Terms of Use Agreement, MYSPACE (June 25, 2009), http://www.myspace.com/Help/Terms (“MySpace . . . is a social networking platform that allows Members to create unique personal profiles online in order to find and communicate with old and new friends.”).
156 See Doninger v. Niehoff, 642 F.3d 334, 344–51 (2d Cir. 2011) (applying students’ First Amendment Rights to speech over the Internet); Steven Greenhouse, Labor Board Says Rights Apply on Net, N.Y. TIMES, Nov. 9, 2010, at B1 (discussing litigation over a worker’s right to criticize her boss on Facebook).
157 John Patzakis, Facebook Spoliation Costs Lawyer $522,000; Ends His Legal Career, EDISCOVERY L. & TECH. BLOG (Nov. 15, 2011, 9:10 PM), http://blog.x1discovery.com/2011/11/15/facebook-spoliation-costs-lawyer-522000-ends-his-legal-career (describing the case of an attorney who
Furthermore admitting evidence from email and social networking profiles will place a burden on the opposing party to refute the credibility of the evidence. Trial preparation is already onerous and having to track down who had access to a particular individual’s account and all those who have posted photographs or other information may prove particularly difficult. In addition, attorneys, as always, may have a tough time earning potential witnesses’ cooperation.

The last and most obvious implication of admitting email and SNS evidence is the possibility of unfairly prejudicial information coming into trials. The purpose of the hearsay and authentication rules is to afford the accused protection. Judges’ roles will expand as they become charged with balancing the probative nature of email and SNS evidence against the potential prejudicial effects.

VII. CONCLUSION

Those who believe that the Internet is a source of “innuendo” and is “inherently unreliable” must recognize the value of email and SNS evidence, which can be a crucial aide in every phase of the legal process. Courts should not bar this important evidence from trial simply because it can be easily edited.

It is clear that there are many ways to authenticate email and SNS evidence. The problem is the lack of a uniform standard across the different jurisdictions. Those jurisdictions that require an exhaustive amount of evidence to prove authenticity may be depriving a party of highly relevant information. On the other hand, jurisdictions that have a low threshold for evidence, such as those which deem email and SNS evidence to be self-authenticating, may improperly burden one side with highly prejudicial evidence. The key is to find a balance, just as the drafters of the Rules did with similar exceptions outlined in Rule 901.

Email and SNS evidence is not inherently different from many of the traditionally accepted forms of evidence. Courts have long accepted potentially forged signatures, letters that were possibly written in another’s handwriting or on another’s computer, and correspondences written on stolen or counterfeit company stationary.

Further, email and SNS evidence is potentially more reliable than other forms of evidence because it is stored on a restricted database and only accessible by those who know the password associated with the account.

told his client to delete photos in fear that they would influence his wrongful death case; the attorney should have attempted a proper legal hold instead of instructing his client to delete the evidence).

158 See Chambers v. Mississippi, 410 U.S. 284, 298 (1973) (“The hearsay rule, which has long been recognized and respected by virtually every State, is based on experience and grounded in the notion that untrustworthy evidence should not be presented to the triers of fact. Out-of-court statements are traditionally excluded because they lack the conventional indicia of reliability . . . .”).
As compared to telephone conversations, for example, email and SNS evidence is more reliable because it is written down and not susceptible to translation errors. Regardless of whether one form or communication is more trustworthy than another, the credibility of evidence has always been a question for the trier of fact—provided the proponent of the evidence makes a showing that the evidence is what it purports to be. Courts should not treat email and SNS evidence differently.

The creation of email and SNS already has significantly affected the legal system. The new challenge is to draft rules that incorporate these forms of communication in an effective and efficient manner. The introduction of videos and photography required a new amendment to the Federal Rules of Evidence; email and SNS evidence warrant an amendment as well. While some courts feel that a new rule is not necessary, a virtual records exception would guide attorneys in their quest for authentication and foster uniformity among the courts.

159 See Chesapeake & Ohio Ry. Co. v. Martin, 283 U.S. 209, 216 (1931) ("We recognize the general rule, of course, as stated by both courts below, that the question of the credibility of witnesses is one for the jury alone.").