American University Criminal Law Brief

Volume 8 | Issue 1 Article 2

Facebook and MySpace in the Courtroom: Authentication of Social Networking Websites

Julia Mehlman

Facebook and MySpace in the Courtroom: Authentication of Social Networking Websites

"As social media, or whatever you want to label it, becomes more prevalent, there will be blunders. We're in experimental mode right now."[2]

"[T]he inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation."[3]

I. Introduction

People reveal their lives online. Since 2005,[4] an entire generation has been archiving its daily, or even hourly, activities for hundreds of followers on social networking websites.[5] Since then, users have continued to multiply, reaching people of all age groups.[6] These sites[7] are "sophisticated tools of communication where the user voluntarily provides information that the user wants to share with others."[8] Many of these sites, including Facebook—the "behemoth of the social networking world"[9]—and MySpace, enable members "to create online 'profiles,' which are individual web pages on which members post photographs, videos, and information about their lives and interests."[10] Users connect by linking their profiles—becoming "friends"— joining similar fan pages, similar networks, "liking" similar things, and sharing content among their accounts.[11]

Although social networking websites have been hugely popular for some time, they are only beginning to find their place in the courtroom.[12] Over the past few years, there has been "an ever increasing number of cases involving social networking communications, and these cases cover a broad range of areas of law."[13] Indeed, social networking websites come up at various stages of litigation, ranging from civil and criminal discovery,[14] to problems with juries,[15] to use as evidence at trial,[16] to sentencing proceedings[17] and beyond.

Although there are problems associated with the use of social networking websites at each of the aforementioned stages, this article focuses on the use of social networking websites as evidence at trial and the problems of authentication, particularly in criminal cases. The article will proceed in three parts. In Part II, this article will address the law of authentication in general, to provide a background for courts' approaches to authenticating social networking websites. In Part III, this article will describe the different methodologies courts use to authenticate different aspects of social networking websites and will compare those approaches to existing case law about authenticating electronically stored information generally. It will begin by examining authentication of messages sent via social networking websites, and then it will analyze postings, photographs, and "tags." Finally, in Part IV, this article will conclude with a summary of the approaches, accompanied by some recommendations and strategies for courts and parties for authenticating this growing category of potential evidence.

In addressing the issues that arise with the authentication of information from social networking websites, most courts begin by looking at the general framework for authentication, focusing on electronically stored information in particular.[18] Some courts feel comfortable applying the existing authentication rules to social networking evidence,[19] while others seem hesitant about the reliability of such evidence, and as a result, heighten existing authentication requirements.[20]

A. Law of Authentication in General

The Federal Rules of Evidence direct trial courts to apply a sufficiency standard to determine whether a document is authentic: the proponent of the evidence must produce evidence sufficient to support a finding that the writing is what the proponent claims it to be.[21] There only needs to be a prima facie showing of authenticity to the court to demonstrate that a reasonable juror could find the document to be authentic.[22] "Once a prima facie case is made, the evidence goes to the jury, and it is the jury who will ultimately determine the authenticity of the evidence instead of the court."[23] Authentication is simply an aspect of relevancy.[24] The proponent's assertion that the writing is relevant determines what he claims the writing to be.[25]

Appellate courts give substantial deference to that determination, reviewing a lower court's decision only for an abuse of discretion, in which the determination is not to be disturbed absent a showing that there is *no* competent evidence in the record to support the decision.[26] According to Federal Rule of Evidence 901(a), documents must be properly authenticated "by evidence sufficient to support a finding that *the matter in question is what its proponent claims*" as a condition precedent to admissibility.[27] If the document is found admissible, it may be relevant. Most state evidence codes echo the wording of Federal Rule 901.[28]

The traditional justification for authentication requirements is to prevent fraud or mistake.[29] For example, consider a set of documents purported to be a series of threatening letters signed by the defendant in a criminal case. The requirement to authenticate—or prove—that the letters were actually signed by the defendant protects him from the possibility that a third party forged the letter to have the defendant arrested or imprisoned for stalking. Authentication also protects that same defendant from the risk that the letter may have been signed by another person with the same name. Beyond the need to prevent mistake and fraud, authentication also serves to provide context to the jury, without which, any given document may be confusing or misleading.[30]

On the other hand, critics of the authentication requirement complain that it demands "proof of what may correctly be assumed true in 99 out of 100 cases," and makes the process "at best time-consuming and expensive[ ]" and at "worst . . . indefensible."[31]

There are many different ways to authenticate evidence, based both on the nature of the document and the purpose of its use.[32] In fact, the Federal Rules allow for authentication methods not explicitly considered in the Rules themselves. For example, although Rule 901 provides some examples and illustrations for ways to authenticate some types of documents, it also explicitly states that the list is not exhaustive.[33] Rather, Rule 901 was purposefully drafted to provide flexibility and allow for the authentication of forms of evidence that the drafters could not have anticipated.[34]

In order to authenticate a document, the proponent of the evidence must first establish what type of document the proffered evidence purports to be.[35] This, however, is generally obvious from the document itself and requires no more than a witness' clarification, for example that the document is a letter,[36] a ledger,[37] or a photograph.[38] The document's role, and its admissibility, more often hinges on other inferences about the document.[39] Examples of such inferences are: Who wrote it?; Who sent it?; Who received it?; Was it altered? The answers to each of these questions determine whether or not the document is relevant.

Rule 901's most typical method of authentication is identifying the author of the document.[40] This, of course, is merely part of the document's relevance.[41] The easiest way to identify the author is to have a witness with personal knowledge authenticate the document by testifying either that he authored it, or for automatically created electronic documents, that he is familiar with the computer processes that created it.[42] However, such testimony is not always feasible and is never required.[43] Rather, a document's author *may* be identified to meet the authentication threshold merely by "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances."[44]

Indeed, circumstantial evidence alone is often enough to satisfy the low authentication bar.[45] For example, the Third Circuit found that the defendant sufficiently established himself as the author of a letter for authentication purposes where the letter was seized from the trash outside his house.[46] The notes were contained in the same garbage bag as other identifying information, and they were written on the stationery of a hotel where the defendant had stayed.[47] Another example comes from the Fourth Circuit, in which the court found that the author was sufficiently identified for authentication purposes where the documents were found in military headquarters with indexing numbers unique to the organization reported to have created the documents.[48] Every other Circuit has also followed this circumstantial authentication approach.[49] It is clear that courts are willing to infer authorship of a document for the purposes of authentication through circumstantial evidence alone.

In addition to authorship, relevance can also be established solely by identifying the person who received or found a document in question.[50] Whether a person received a document can be important in establishing that person's knowledge of or reaction to the information contained therein, or the fact that he was in communication with a given person.[51] Inferring that a person received a document can be accomplished through direct testimony from that person, since that individual would have personal knowledge of the communication.[52] Once again, however, such testimony is not always feasible and is never required.[53] Rather, circumstantial evidence will often suffice.[54] For example, the fact that an individual showed up at the exact

location and time mentioned in the document, was sufficient to authenticate that he had received the message.[55] Thus, circumstantial evidence that an individual "must have read" the document can be enough for authentication.[56]

Another inference the court must make before determining that a document is properly authenticated, is finding that the document has not been altered from its original state.[57] This is especially important for photographs, which, although they are sometimes included in the category of writings, have some distinct authentication rules in case law.[58] There are two separate issues that must be addressed in the authentication process for photographs: first, what the scene is that the photograph depicts; and second, whether the photograph is an accurate representation of that scene.[59] With respect to the first issue, a picture may be inadmissible because it fails to show the object, place, or person in question, but also may be "inadmissible, although technically accurate, because it portrays a scene that is materially different from a scene that is relevant to one of the issues at trial."[60] For example, if someone materially altered the scene itself, even if it were the correct scene, authentication would be barred.[61] A photograph may also be inadmissible because it has been altered or distorted and thus is "inadmissible as a technically inaccurate representation of the scene photographed."[62]

The problems associated with authenticating photographs became even more complicated with the popularization of digital photography.

The problems associated with authenticating photographs became even more complicated with the popularization of digital photography.[63] The rise of digital photography has also prompted the creation of technology that alters images in subtle ways; in many cases, these subtle alterations have not affected the admissibility of the images.[64] For example, in *United States v. Seifert*, an arson case, the Eighth Circuit dealt with surveillance videotape from a building security system.[65] The surveillance videotape was filmed at a slower than normal speed in an extra-small, extra-dark format.[66] To aid the jury in viewing the videotape, the prosecution enhanced the videotape in three different ways: (1) speeding up the frames to make it look like "real time," (2) enlarging each frame to full-screen size, and (3) brightening the film.[67] These alterations did not bar authentication because they "[did] not change the image, but assist[ed] the jury in its observation and viewing of the image, which [enhanced] their understanding."[68]

In *United States v. Beeler*, the government also sought to introduce surveillance videotape that was duplicated and enhanced.[69] Alterations just like those in *Seifert* were made to the surveillance videotape.[70] Likewise, in *Beeler*, the court found that the edited and enhanced version of the videotape was an "accurate, authentic, and trustworthy representation[] of the original" and admitted the tapes.[71] Thus, *some* digital alterations are acceptable. One can imagine other digital processes that are possible on computer systems, but unacceptable for purposes of authentication, like "photoshopping"[72] an object or individual into the scene that was not there before.[73] Such processes are easy to do with digital photography.

The above, well-established, case law regarding authentication of hard-copy documents and photographs has become more important as a baseline for courts to use in addressing a new genre of documentary evidence: information stored on computers or on the internet. In *Lorraine v. Markel American Insurance Company*, the District Court of Maryland noted that authentication of documents from a computer, often called electronically stored information, or "ESI," may require greater scrutiny than that required for the authentication of hard copy documents.[74] The *Lorraine* court surveyed ESI authentication cases from across the country[75] and concluded that admissibility of ESI is "complicated by the fact that ESI comes in multiple evidentiary 'flavors,' including e-mail, website ESI, internet postings, digital photographs, and computer-generated documents and data files."[76]

Still, the *Lorraine* court found "no justification for constructing unique rules of admissibility of electronic communications" because "the same uncertainties exist" in ESI as in hard copy documents.[77] Those uncertainties echo the above discussion about the inferences required to authenticate a document: with ESI, the author may be difficult to identify given the fact that multiple users may have access to the information, which makes it more difficult to confirm whether the information has been sent or received by a particular person, and advanced computer technology makes alteration more likely.[78] Moreover, most attempts to introduce ESI into evidence are through the use of hard copy printouts of the electronic information.[79] This means that the printouts themselves must be authenticated as "accurately reflecting the content of the online page and the image of the page on the computer at which the printout was made."[80] Despite this added complexity, courts have adapted a flexible and comprehensive framework to address authenticating ESI based on the same core concepts used for authentication in general.[81] These core concepts include identifying the author or creator, identifying the person who received the document, and determining whether the document is an accurate representation of a person, place, or thing.[82]

B. Authenticating Social Networking Websites

Social networking websites have many features that parties have sought to enter into evidence at trial.[83] Such evidence includes: (1) personal messages sent via social networking websites; (2) postings on an individual account holder's web pages; (3) photographs posted on an individual's account or web page; and (4) "tags," in which one account-holder lists another individual's name to indicate that that person is in a photograph, at an event, or simply has something to do with a comment.

Further, as is the case with the many types of documents subject to authentication, the different parts of social networking websites each present unique problems for authentication. Most of these problems can be addressed by using the same set of inferences used for authentication in general. Of course, if the person who is alleged to have sent the message, posted the information, appeared in the photograph, or otherwise made the statement, simply testifies to his personal knowledge that he sent it, posted it, or was present at the scene, then the inquiry ends there, and the exhibit—most often a hard copy print-out of electronic information—is authenticated.[84] However, in many circumstances, the person against whom the document is offered will not testify or will deny creating the document.[85] In such cases, the myriad types of ESI that might be introduced and the ways to authenticate this diverse category of evidence "underscore[] the need for counsel to be creative in identifying methods of authenticating" the evidence.[86]

1. Messages

One of the many functions of social networking websites is to provide an online forum for the communication of messages. These websites allow users to sign into personal accounts and send messages to other individuals who have accounts on the same website. Like email, the messages are electronic communications sent from a given account with a clear timestamp. Like email, the user must provide the correct password in order to access the account and send a message. Also like email, the user may choose to send the message to a single receiver or to a specified group of recipients. In developing an approach to authenticate Facebook and MySpace messages, courts have looked to e-mail and other electronic communications as either a model to be followed or a starting point from which to embark on the path to authentication.[87]

In its survey of ESI authentication across the federal system, the District Court of Maryland noted that "[t]he most frequent ways to authenticate e-mail evidence are 901(b)(1) (person with personal knowledge), 901(b)(3) (expert testimony or comparison with authenticated exemplar), [and] 901(b)(4) (distinctive characteristics, including circumstantial evidence)."[88] Indeed, all three of these methods are used to authenticate internet postings in general.[89] Once again, because identification of the author basically determines whether the exhibit is relevant, it is the most important inference in a message. Importantly, however, when it comes to the author or sender of an e-mail, "the sending address in an e-mail message is not conclusive" because someone with unauthorized access to an account —or even an authorized user acting outside the scope of the authorization he was given—could always send an e-mail in the account owner's name.[90] The same possibility—that someone other than the account holder could send a message without the account holder's authorization—is present and prevalent with messages sent from social networking accounts.

Existing case law[91] indicates that courts have generally taken one of three approaches with respect to authenticating messages sent on Facebook and MySpace. The first approach likens social networking website messages to e-mail and requires no further information to authenticate messages than what is required for email.[92] The other approaches go a step further and require either testimony about the distinctive nature of the messages' content,[93] the security settings of the social networking website,[94] or both.[95] This article refers to these other approaches as the corroboration approach, the security approach, and the combined approach, respectively.

i. The E-mail Parallel Approach

The first approach requires little information to authenticate messages sent from Facebook, MySpace, and other similar sites. One example of this more lax approach is *People v. Clevenstine*, a rape case in which an appellate court in New York found sufficient authentication of MySpace messages based on nothing more than the fact that the messages were sent from the defendant's account.[96] Referring back to the existing e-mail framework, this is the equivalent of finding an e-mail's author sufficiently identified for authentication, solely because it was sent from that individual's e-mail address.

In *Clevenstine*, the prosecution sought to introduce MySpace messages sent from the defendant to an alleged rape victim.[97] The defendant did not testify.[98] Testimony about the MySpace messages included the following: the defendant's wife found the messages on the defendant's computer, and she recalled the content of the communications; the police retrieved a record of the messages from the victim's hard drive, which meant the messages were written from his computer; and a MySpace legal compliance officer testified that the defendant had created the sending account.[99] The *Clevenstine* court found that to be sufficient for authentication.[100]

The court recognized the possibility that someone else could have accessed the defendant's MySpace account, but held that "the likelihood of such a scenario presented a factual issue for the jury," rather than a bar to authentication.[101] There was no testimony about whether the content of the messages was

information only the defendant would have known, or whether the writing style resembled his.[102] Despite recognizing the potential risk that the defendant had *not* written the messages in question, the court found them sufficiently authenticated for admission into evidence.[103] Thus, the *Clevenstine* approach deemed messages authentic despite the presence of unanswered questions, which, as discussed below, other courts have considered highly relevant.[104]

ii. The Corroboration Approach

Courts following the other two approaches require something beyond unsubstantiated testimony that the account belongs to the defendant and that the messages were written from the defendant's computer.[105] These two approaches can be classified as: (1) the corroboration approach; and (2) the security approach, which requires testimony about the security procedures in place for the social networking website.[106] The rigorous corroboration approach is similar to the process of authenticating e-mails through circumstantial evidence; e-mails are often deemed authenticated as to authorship by inclusion of factual details known only to the individual to whom the message is attributed along with some other corroborating evidence.[107] Insofar as e-mail is concerned, the Fifth and Eleventh Circuits, and various district courts have followed this approach.[108]

The simplest corroboration approach focuses only on the content of the messages. In such cases, courts explicitly rely on authentication practices for e-mail and draw analogies to messages sent via social networking websites.[109] For example, in *Manuel v. State*, a Texas court dealt with MySpace messages in a stalking case.[110] In determining whether the proffered information identified the defendant as the author, the court noted that in *Massimo v. State*, e-mails were authenticated where, *inter alia*, (1) a witness recognized the e-mail address as belonging to the defendant; (2) the e-mails discussed information only the victim, defendant, and a few other people knew; and (3) the e-mails were written in a way the defendant was known to communicate.[111]

The *Manuel* court reviewed the content and writing style of the many messages sent to the victim via MySpace and based on the case law for authenticating e-mail in *Massimo*, concluded that the content was distinctive enough to tie the defendant to the message in such a way that a reasonable fact finder could conclude that the defendant sent all of the messages.[112] This was especially true in *Manuel* because other evidence corroborated information in the MySpace messages. For example, in one message the sender discussed giving the victim a ring, and later gave a ring to a friend to deliver to the victim.[113] This corroboration requirement has existed for e-mail authentication for over a decade.[114] Courts now treat this corroboration requirement as an established principle for e-mails; most frequently, identification of authorship through the e-mail address must be corroborated by other authenticating factors, like content, circumstances, internal patterns, and extrinsic evidence.[115]

Instead of wholesale adoption of the e-mail approach, some courts combine both the security and corroboration approaches, resulting in the most burdensome approach to authenticating social networking messages.[116] One example of a court following this combined "security and corroboration approach" is *State v. Eleck*, an assault case in which defense counsel sought to admit messages allegedly sent by a witness from her Facebook account to the defendant's Facebook account.[117] The witness, who was called by the state, testified that prior to the assault the defendant stated to her, in person, that "if anyone messes with me tonight, I'm going to stab them."[118] On direct, she testified that she had not spoken or communicated with the defendant either in person or on the computer since the incident.[119] Defense counsel sought to impeach the witness by showing that she had been in touch with the defendant since the incident through Facebook messages.[120]

The defendant sought to introduce purported Facebook messages between the defendant and the witness in order to impeach the witness, who denied having spoken with the defendant in person or on the computer since the assault.[121] To authenticate the messages, the defendant took the stand and reported downloading and printing the messages from his computer.[122] He further identified photographs and other postings on the account that suggested that the witness was the owner of the account.[123] The witness herself even admitted that the username was hers and she was the true account owner, but she denied sending the messages.[124] She testified that someone hacked into her account and changed her password, so she no longer had access to the account.[125] Specifically, she asserted that the account was hacked two weeks before her testimony—not at the time the messages were sent.[126]

Although this situation appears to be a traditional credibility dispute, which would present a question for the jury under the sufficiency standard discussed above, the trial court did not treat it that way. Instead, the trial court excluded the messages, and the appellate court affirmed, finding insufficient information to authenticate that the witness wrote the Facebook messages.[127] The court found that the parties established that the messages came from the witness' account, but not that she had, in fact, written and sent them.[128] Thus the court concluded that the messages were inadmissible.[129]

The *Eleck* court noted that while the traditional rules of evidence likely provided a sufficient framework for authenticating such messages, there needed to be some sort of circumstantial evidence to establish that the named sender was the actual author.[130] In fact, the court gave several examples of the type of corroborating information that could have been used to authenticate the sender of the messages.[131] One example was showing that the content on the sender's account established the

author's identity.[132] Another was showing that the information included in the messages was known solely to the alleged sender.[133] That information, the court noted, must be "distinctive of the purported author and . . . corroborated by other events or with forensic computer evidence."[134] The court found that the messages' mere suggestion of acrimonious history between the witness and the defendant was not sufficiently distinctive to establish the defendant as a sender because other people could have known about it.[135] In other words, these messages did not pass muster under the corroboration approach.

The court also suggested searching the computer's internet history,[136] presumably referring to IP address[137] information, to show that the user signed on *from that computer*.[138] Although the court recognized that the possibility that the witness' account had been hacked was "dubious"—especially given that the messages were sent prior to the alleged hacking—the court still found that there was insufficient foundation that she had authored and sent the messages herself.[139] In short, the court found that the messages were not authenticated under the security approach, either.[140]

The *Eleck* court set a higher bar for the authentication of messages sent from social networking websites than did the *Clevenstine* court in New York.[141] *Eleck* specifically mentioned that social networking websites suffer from a "general lack of security" which "raises an issue as to whether a third party may have sent the messages."[142] Perhaps in addition to meeting the low sufficiency standard for relevance under Rule 401 and the slightly higher sufficiency standard for authentication under Rule 901, the *Eleck* court—without explicitly saying so—imported concerns normally dealt with under Rule 403, which include "unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence."[143] Absent this implicit move, it is difficult to understand why the *Eleck* court did not simply mirror the requirements of e-mail authentication.

The rigorous corroboration approach is similar to the process of authenticating e-mails through circumstantial evidence; e-mails are often deemed authenticated as to authorship by inclusion of factual details known only to the individual to whom the message is attributed along with some other corroborating evidence.

iii. The Security Approach

Among the requirements the *Eleck* court demanded to meet its heightened standard was testimony about the security procedures in place for social networking websites.[144] This court was not the first to do so. In fact, other courts have not just suggested this approach in dicta, but have actually used it.[145]

The *Eleck* court relied on a recent Massachusetts case in which a court held that proof that a MySpace message came from a particular account, without further authenticating evidence that a particular person actually wrote it, was inadequate proof of authorship.[146] In that case, *Commonwealth v. Williams*, the prosecutor entered into evidence MySpace messages sent from the defendant's brother's account, and the defendant unsuccessfully moved to strike the messages.[147] The appellate court found that the messages were not authenticated because there was insufficient information identifying the sender.[148] As the *Eleck* court later echoed, *Williams* highlighted the need for information about the website's privacy and security measures–"[a]though it appears that the sender of the messages was using [defendant's brother's] MySpace Web 'page,' there is no testimony . . . regarding how secure such a Web page is, who can access a MySpace Web page, whether codes are needed for such access, etc."[149]

Therefore, the security approach represents a big leap forward from the traditional authentication process, requiring information about security procedures, customarily absent from authentication of e-mails.

iv. Summary and Recommendations

Based on the above cases, there appears to be three different approaches to authenticating messages sent from social networking websites. The first, which is the lowest hurdle, requires information showing that the messages were sent from the user's account. This approach considers the risk that a third party hacked into the account as going to the evidence's weight and not its admissibility. The next two

approaches require something *beyond* proof that the messages were sent from a given account to establish authorship. The corroboration approach follows the courts' procedure for e-mail authentication, looking to the distinctive nature of the content or other corroborating information to show authorship. The security approach goes beyond the established approach to e-mail, calling for proof regarding the social networking websites' privacy and security settings. The combined corroboration and security approach requires both.

Although there is little case law addressing this issue to date, there is some indication that the approach to authentication varies depending on how vital the piece of evidence is to the case and on how severe the charges are.[150] Where the case truly hinges on a certain message, more details are required to establish authorship. For example, in *Clevenstine*, the rape case, the messages from the defendant to the victims were of secondary importance, given that the victims' testimony about the rape itself was more integral to the case.[151] Accordingly, the court deemed the messages authenticated despite the recognized risk that the defendant may not have sent them.[152] By contrast, in *Eleck*, the assault case, the message went to the defendant's intent to harm, which was key evidence; accordingly, that court required extra evidence to establish authorship.[153]

Courts have yet to explain the underlying justification for raising the bar for authentication when it comes to messages sent from social networking websites rather than from e-mail accounts.[154] There is no reason for the heightened requirement of discussing the websites' security settings. The security settings are similar—both are password-protected; to access the account, an individual must enter an accurate username and password. The expectations of user privacy are also similar in that both are private messages from one sender to a particular receiver that are not publicly displayed. With respect to the concern about hackers, both an e-mail account and a social networking account can be hacked into—no court has offered information about why it would be more likely to occur in the social networking context.[155] To that end, parties seeking to admit such messages should explain to the court that there is no real difference between sending a message from a social networking website versus an e-mail account. Parties seeking to admit this type of evidence should remind the court that the messages are, in purpose and in effect, no different from e-mail, which is routinely authenticated and admitted into evidence.[156]

In contrast, parties seeking to exclude messages from social networking websites should rely heavily on *Eleck*'s corroboration and security approaches.[157] It would be useful to call an expert witness prepared to discuss the fallibility of Facebook and MySpace password protection, impressing on courts the ease with which third parties can hack into a user's account.[158] Beyond infiltrating another user's account, parties seeking to exclude this evidence should also explain to the court the all-too-common practice of creating fake accounts on social networking websites, in which people create accounts in other people's names.[159]

To counter such an approach, the proponent of the evidence must come to court with his own witness familiar with the security settings.[160] This, however, could mean that the security-driven approach may lead to a battle-of-the-experts, which would be an undesirable outcome on two fronts. First, a battle-of-the-experts could risk losing the jury's attention, adding needless time to each trial, and decreasing the jury's comprehension. Second, it could decrease the perceived fairness of the proceedings, particularly for indigent criminal defendants, who most likely will not be able to afford to hire this type of expert. Although *Eleck* used the corroboration approach, the opinion called for security testimony as well.[161] Perhaps in recognition of the undesirability of this outcome and the questionable need to distinguish these messages from e-mail, the Connecticut Supreme Court recently granted certiorari on the limited issue of authentication of the Facebook messages.[162]

In sum, the various approaches to authentication of messages sent from social networking websites have the potential to lead to quite different trial records and outcomes. These messages appear to be, for all intents and purposes, nearly identical to e-mail messages. Some courts resist the comparison and require a higher threshold of evidence to authenticate, but they do so without providing a meaningful distinction between the two types of messages. Whether or not the *Eleck* approach will remain good law in Connecticut will, perhaps, determine the trend in jurisdictions across the country.

2. Postings

In contrast to messages sent on social networking websites, wall postings on these same websites are quite different from e-mail. In addressing authentication of wall postings, courts tend not to analogize to e-mail at all, but rather to postings on other public forums on the web.[163]

Internet postings constitute a complex category that includes "data posted by the site owner, data posted by others with consent of the site owner, and data posted by others without consent, such as 'hackers.'"[164] Reactions to internet postings in court have ranged from "famous skepticism" to a "more permissive approach[.]"[165] When it comes to postings on social networking sites, there are even more subdivisions to add: data posted on one's own wall by the account owner, data posted on the account owner's wall by other users, and data posted in various groups or forums by an account user.

The "wall" or "page" generally refers to a public space on an individual's account homepage, or "profile page," where information can be posted for viewing. The account user determines which people can view the information posted on his wall. The user can allow universal access to the information,

or he can limit access to defined groups: people in the same regional network, people from the same school, people he is "friends" with on the website, and individuals with whom the user has acknowledged a relationship. Given the various privacy settings, "Facebook wall postings and the MySpace comments are not strictly 'public,' but are accessible only to those users [the account holder] selects."[166] In practice, such postings can "be viewed by anyone with access to the user's profile page."[167] Moreover, "[a]lthough a social networking site generally requires a unique username and password for the user to both establish a profile and access it, posting on the site by those that befriend the user does not."[168]

As with messages, the principal inference concerning the authentication of wall posts is *who* wrote the post—was it really the account holder to whom the post is attributed, or did someone else write it?[169] Because of its novelty, courts have had little opportunity to address this issue. However, the issue has reached one state supreme court, which highlights its importance.[170]

In *Griffin v. State*, a murder case, the Maryland Supreme Court dealt with authenticating posts on the MySpace profile page allegedly belonging to the defendant's girlfriend, witness Jessica Barber.[171] The trial court admitted hard copy printouts of her alleged profile page.[172] The prosecution sought to use posts on her profile page to demonstrate that Ms. Barber had threatened another State witness in an apparent attempt to prevent that witness from testifying against the defendant.[173] The post contained some identifying information that connected the page to Ms. Barber, including her birthday, gender, and hometown.[174] Notably, the page also contained a threatening post: "FREE BOOZY!!!! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"[175]

When she took the stand, Ms. Barber was not questioned about the pages allegedly printed from her MySpace profile.[176] Instead, the State sought to authenticate the profile posting solely through the testimony of the lead investigator in the case, Sergeant John Cook.[177] In lieu of his testimony, the parties entered a stipulation that the investigator logged onto MySpace and found the profile page with a photograph that resembled Ms. Barber along with the identifying information listed above, which is why he believed it to be her account.[178] The parties further stipulated that the statement in question was posted on that profile page.[179] The court concluded that this stipulated information established that the profile page belonged to Ms. Barber, but did not address whether she actually had authored the threatening post.[180] This is because the court was concerned that, despite the identifying information, the profile may not have been Ms. Barber's at all.[181]

Among the issues discussed in *Griffin*, the court focused on the fact that people viewing a MySpace page have no idea whether the information is real or not. "A person observing the online profile of a user with whom the observer is unacquainted has no idea whether the profile is legitimate."[182] The court's great concern was two-fold: first, that someone could "create a fictitious account and masquerade under another person's name[;]"[183] and about the potential for hackers—people who "gain access to another's account by obtaining the user's username and password[.]"[184] In short, "[t]he potential for fabricating or tampering with electronically stored information on a social networking site . . . poses significant challenges from the standpoint of authentication of printouts of the site[.]"[185] Bringing it back to the facts at hand, this means that while the content posted on the page was certainly a threat, it may not have been real—someone could have faked the entire profile, and, accordingly, faked the threat. Acknowledging its unfamiliarity with social networking websites, as in the messaging cases, the *Griffin* court turned to authentication of other types of ESI for guidance.[186] But, given the concerns mentioned above, the *Griffin* court concluded that from a policy perspective, postings require "greater scrutiny [than typical ESI] because of the heightened possibility for manipulation by other than the true user or poster."[187]

In *Griffin*, the court concluded that there are two stages at which authentication of authorship is required for wall postings: first, the proponent of the evidence must show that the alleged account holder—here, Ms. Barber—is really the person who created the account; and second, the proponent must show that the account holder is also the author of the post in question.[188] As in *Eleck*, the *Griffin* court suggested various ways to authenticate postings on social networking websites: (1) having the author admit to writing the post in question; (2) searching the author's computer to examine whether the website was accessed from that computer; or (3) getting information from the social networking website linking the profile and the post to the alleged author.[189] Some sort of "extrinsic evidence" is needed.[190] However, even those methods do not foreclose the possibility that another person accessed the witness' account and computer.

In *Griffin*, the lower court found that the officer's testimony about the photograph, the correct birth date listed on the profile page, as well as the rest of its content, sufficiently linked the page to Ms. Barber.[191] Ultimately, the Maryland Court of Appeals reversed the lower court and found that the pages were not properly authenticated and should not have been admitted into evidence.[192] No petition for review has been filed with the Supreme Court to date, despite the dissent's characterization of the majority's treatment of Facebook postings as "technological heebie jeebies[.]"[193]

The two dissenting judges in the *Griffin* appeal case found that the identifying information in the messages considered by the majority was actually sufficient for a reasonable juror to conclude that the information was authored by Ms. Barber.[194]

[P]eople may write wall postings that simply do not reflect their thoughts, feelings, or behaviors in the world beyond the web. Accordingly, it would behoove parties seeking to exclude such information to explain to the courts that even if authorship were established, the information is still not relevant because it is not an accurate reflection of any person's true state of mind or intent.

With respect to the majority's fear that hackers, rather than the account holder, authored the messages, the dissent did not consider that fear in the abstract, but rather looked at the record, which they found "suggest[ed] no motive" for anyone to do so.[195] According to the dissent, any lingering threat that a hacker had authored the messages should go to weight, not admissibility, and should be dealt with through cross-examination.[196] Thus, the *Griffin* dissenters' approach added no extra burden and more closely paralleled typical e-mail authentication. Nevertheless, the *Griffin* majority's more burdensome standard remains good law.

Beyond *Griffin*, in which a witness allegedly posted information on her *own* profile page, lies a situation yet to be considered by any court. In this scenario, a social networking website user posts information on another individual's profile page or wall. Here, the danger of hackers posting information while the user remains unaware is much higher. In the *Griffin* context, if a hacker posted information on the user's own profile page, it is reasonable to conclude that the user would eventually come across that information. After all, the information is posted on his own account. By contrast, if a hacker logs in to a user's account and posts on a different individual's wall, the user may never learn of the post.

To demonstrate this problem, consider a variation of the facts in *Griffin.* Assume, for the sake of illustration, that the account in question in fact belongs to Ms. Barber. Now, assume the account is hacked. Instead of posting a threat to the prosecution's witness on Ms. Barber's own profile page, the hacker logs into Ms. Barber's account, clicks to view the other witness' profile, then posts the threat on that witness' profile page. Ms. Barber may never learn that the hacker authored such a post on the other person's page, unless she logs into her own account and decides to view that person's profile page herself. No court has dealt with this issue yet, but it presumably adds yet another step to the authentication process for postings.

As in messaging, then, the possibility of hackers is a hurdle that potentially blocks authentication of wall postings.[197] This hurdle is even more apt for wall posting because the account holder may never learn of information posted on someone else's wall from his own account; until recently, unlike messages there was no "outbox" that kept a record of outgoing posts the way there was for outgoing messages. Therefore, the risk of hackers has been treated as preempting a finding of facts sufficient for authentication even when the posting is on the purported author's own "wall." In *Griffin*, that risk was allocated to the proponent of the posting, and the court put the onus on the proponent to somehow reduce the risk in order to satisfy the sufficiency standard.[198]

Moreover, in the situations described above—information posted on one's own profile or on another user's wall or page—another real problem is the content of the information posted. Even if authorship is established, the relevance of the post may be questionable.[199] At least in *Griffin*, the post was offered to prove the truth of the matter asserted in the post.[200] The court was attempting to use that post to show that she had threatened another witness.[201] This indicates that courts are treating assertions on social networking sites as true statements. Research outside of the legal field suggests that this is not exactly a reliable approach, because "[b]eing able to communicate in a faceless manner [through social networking websites] from the comfort of one's own living room tends to make people bolder than they are in real life."[202] This means that people may write wall postings that simply do not reflect their thoughts, feelings, or behaviors in the world beyond the web.[203] Accordingly, it would behoove parties seeking to exclude such information to explain to the courts that even if authorship were established, the information is still not relevant because it is not an accurate reflection of any person's true state of mind or intent. Still, "the standard of authentication is relatively low," so the evidence may come in despite such warnings.[204]

Of course, the above discussion is simply a prediction, since only the *Griffin* court has addressed this issue. Whether other jurisdictions decide to follow the *Griffin* court's lead, or the self-proclaimed more technologically savvy dissent, whose approach parallels e-mail authentication, will shape the litigation practice regarding postings on social networking sites.

3. Photographs

In addition to providing a forum for communication of messages and public posting of information, social networking websites also serve as online, shareable photo albums. First, each individual user can post a "profile picture," which is shown on the user's profile page. When the user posts on other profiles, groups, or sends a message, his chosen profile picture appears alongside the message. Users can change their profile pictures whenever they want, and old profile pictures are gathered in a lasting album on the user's page. Beyond profile pictures, social networking websites allow users to upload photographs to create albums to share with others. There is no limit to the number of photographs that users may upload and share. On every photograph, the user has an option to create a caption. Other users given permission to view the album can also post comments to each photograph or to the album as a whole.

Some social networking websites, like Facebook, have a feature that allows users to "tag" their friends in pictures. Essentially, a tag is a way to identify who is in the picture. If a user's account is tagged in a picture, he will receive notice. However, there is no photo-recognition technology that notifies a user whenever a photo of him has been shared on Facebook. Moreover, if the person has tagged another user improperly—using the wrong spelling, for example—the user will not be notified that the photograph has been posted.

There is no feature on social networking websites that monitors the content of the photograph and there is no way to determine if whatever caption posted to the photograph is accurate. Further, there are only minimal tools available for alerting the websites to inappropriate or inaccurate photographs. For example, on Facebook the user has an option to "report" a photo to the website administration. The user is limited to two categories for reporting a photograph: that the photograph is a picture of the user and the user either does not like the photo or finds it to be harassing; or that the photograph is not of the user, but rather is "spam or scam, nudity or pornography, graphic violence, hate speech or symbol, illegal drug use, [or] my friend's account might be compromised or hacked."[205] There is no option available to report that the photograph is inaccurate or altered.

At least two courts have addressed the use at trial of photographs uploaded onto social networking websites and later printed out as hard copies.[206] Both have referred to methods of authenticating photographs in general.[207] Photographs are usually authenticated "by a witness with personal knowledge of the scene depicted who can testify that the photo fairly and accurately describes [the scene]."[208]

As described above, authenticating photographs became more complex with the advent of digital photography. As one court explained it, digital photographs "present unique authentication problems because they are a form of electronically produced evidence that may be manipulated and altered."[209] Once digital photographs are uploaded to computers, even with the simplest of programs like Photoshop, concerns exist about people "removing, inserting, or highlighting" particular aspects of the photograph.[210] For that reason, *two* inferential leaps are required to authenticate a digital photograph from a social networking website: beyond determining that the scene depicts what the party says it depicts, the court must also find that a reasonable juror could conclude that the photograph has not been altered in any impermissible way.[211]

In *People v. Beckley*, a murder case, the prosecution sought to admit photographs posted on the defendant's MySpace page.[212] At issue in the case was whether the defendant was a gang member and whether the shooting was part of gang retaliation.[213] The pictures showed one of the defense witnesses flashing gang signs.[214] The prosecution sought to use the pictures to impeach the witness by rebutting her testimony that she did not associate with gang members.[215] The defense conceded that the face in the photograph was in fact a picture of the witness, but still challenged its authenticity.[216]

As a first step, the *Beckley* court looked to case law about authenticating photographs in general, and noted that, like messages and other postings from social networking websites, a photograph is a writing and likewise requires authentication.[217] Beyond the general premise that photographs must be authenticated, the *Beckley* court also highlighted "the untrustworthiness of images downloaded from the internet."[218] Specifically, the court noted that anyone can post a photograph online, that photographs on websites are not monitored for accuracy, that images are not posted under oath, and that hackers can easily adulterate images posted to the web.[219]

Mirroring the need for expert testimony in the context of messages, the *Beckley* court explained that testimony from a photographic expert that the photograph was not a composite and had not been faked is "critical," and could have authenticated the photograph in question.[220] The need for expert testimony for photographic social networking evidence brings up fairness concerns for criminal defendants, echoing the concerns discussed above in the messaging context. It is unlikely that many criminal defendants can afford the fees required to have such expert testimony in court.[221] Because no such expert testified in *Beckley*, the court concluded that the photographs were not properly authenticated and should have been excluded.[222] But, the court found that their admission was merely harmless

error.[223] The *Beckley* court's approach is on par with existing approaches to authenticating digital photographs in general: that the photograph happened to be posted on MySpace did not trigger any additional requirements for authentication.

People v. Lenihan, a murder case in New York, went further than *Beckley*, suggesting that not even expert testimony could solve the authentication problem for photographs found on social networking websites.[224] In *Lenihan* the defendant sought to use photographs printed from MySpace to cross-examine witnesses about their alleged gang ties.[225] Besides the photographs, there was no other evidence of the witnesses' gang membership that could be used to justify the questions on cross-examination.[226] The defendant's mother found photographs on MySpace that allegedly depicted the state's witnesses making hand gestures and wearing clothing that suggested an affiliation with a certain gang.[227] Like *Beckley*, the *Lenihan* court determined that the photographs could not be properly authenticated "[i]n light of the ability to 'photo shop,' [or] edit photographs on the computer[.]"[228] In fact, the court was so convinced that there was no way to authenticate the photographs that it completely barred the defendant from cross-examining the state's witnesses about their gang affiliation and confronting them with the photographs.[229] The *Lenihan* court was so sure that the photographs could not be authenticated that it was willing to bet the defendant's Sixth Amendment Confrontation Clause rights by denying the cross-examination.[230]

These two cases have strong implications for the evidentiary role of photographs uploaded to social networking websites. Despite publicized warnings about keeping questionable photographs off of the internet,[231] the minimal case law here suggests that an individual's online images are not a problem once the case reaches the courtroom unless (1) the witness concedes that the photographs are authentic; or (2) an expert testifies that the photographs have not been altered.[232] Absent these two criteria, social networking website photographs are unlikely to be used against a witness at trial under *Beckley* and *Lenihan*.[233]

Still, social networking website users would be wise to monitor photographs that do end up online, as courts may feel more comfortable admitting such photographs as they become more comfortable with social networking websites in general. Further, the courts in both *Beckley* and *Lenihan* essentially gave instructions for parties seeking to use such photographs as evidence.[234] According to *Beckley*, all the proponent of such evidence must do is hire an expert in digital photography to testify that the photograph is not a composite and that the scene depicted in the photograph on the social networking site had not been altered in a meaningful way.[235] If the *Beckley* court's instructions hold and parties actually follow that advice, then it will not be long before such photographs are routinely entered into evidence.

4. Comments, Tags, and Other Notifications

Courts have had the chance to address the evidentiary use of messages, postings, and photographs from social networking websites, and as described above, the law of authenticating each of those types of evidence will likely evolve over the next few years. In addition to adaptations in their approaches to those three types of evidence, courts will inevitably be faced with evidence in the form of the many other tools and features of social networking websites. Because there is no available case law on the rest of these features, one can only imagine how the courts will handle attempts to use them as evidence. It is helpful to understand the many features of social networking websites before predicting how courts will treat them.

"Tags," in photographs, status updates, or wall postings, have not been addressed in court. "[P]hoto tagging is a popular feature that allows users to identify themselves or other members of the site by name in photos. A photo tag creates a link to that user's profile and identifies the person and her specific location in the photo."[236] Any user can tag another user with whom he is friends in a photo. Although the tagged user has the option to remove her account name—her online identity—from the photograph, the photograph remains on the social networking site until the user who uploaded it chooses to take it down.[237] The initial tagging process is unmonitored, and a user can feel free to tag any part of a photograph as any one of his friends, despite the possibility that the tags may be incorrect.[238]

The tagging process also extends beyond photographs to postings. A relatively new feature on Facebook allows users to tag friends in status updates and comments as well.[239] Likewise, the tag may not be valid, but the post will remain on the site until the user who authored it decides to delete it. Further, in addition to tagging, both Facebook and MySpace allow users to caption or comment on photographs that they post or photographs posted by other people.

Extending courts' logic of authenticating messages and photographs to tagging, the problems only worsen. First, the same susceptibility to hacking exists—in fact, if anything it is even more prevalent with tagging. This is especially true given that unlike messages or photographs, the user may never receive notification that his account posted a comment or a tag on someone else's account. Further, if the user infrequently checks his account, he may have been tagged in countless photographs or comments inaccurately or inappropriately. For example, imagine one user has posted a photograph onto his own Facebook profile page. The photograph depicts a scene at night. It is dark outside. There are several people in the photograph, but their faces are obscured because of the darkness. Although their faces cannot be seen, the metallic glare of guns held in each of their hands can be seen. The user tags a criminal defendant in the photograph. That criminal defendant does not log on to

Facebook anymore, so he receives no notice of the tag. In his prosecution for gang-related crimes, the government seeks to use the photograph against the defendant to show that he had access to a firearm. There are several possible explanations for why the defendant was tagged in that photograph. First, of course, he could have been in the photograph. Second, it could have been a joke—the user could have uploaded a random photograph he found on the internet and tagged his friends in it. Third, it could have been a mistaken tag: the user meant to tag a different friend with a similar name, and wound up tagging the defendant. Because of the myriad possibilities, the meaning of a tag is even less clear than a message or a photograph.

While a tag may indicate that the tagged user is in a photograph, as above, or has participated in some activity with the tagging user, it may also indicate that the tagging user wishes only to get the tagged user's attention. The meaning of a tag in a photograph or comment, then, is speculative at best. Another example illustrates the complexity of this problem. Imagine one user posts a photograph picturing no people, but only guns. Another user tags the defendant in a criminal case in the photograph. There is no indication that the defendant ever received notice of the tag. Certainly there is no way that the tag actually indicates that the defendant is *in* the photograph. Can the state use the photograph to indicate the defendant's connection to firearms? There are many necessary inferences to authentication in this situation. First, who tagged the defendant? The general issues of authenticating the author of any social networking communication apply at this level. Next, what is the photograph intending to depict and has it been altered? The general issues of authenticating a photograph also apply. Finally, what, if anything, is the truth that a tag asserts? Although it seems inevitable that parties will eventually seek to enter such tags as evidence, it seems unlikely that courts will jump through each of these hoops to authenticate such a tag on a social networking website because it would take too much time and energy for very little probative value.

Although it seems inevitable that parties will eventually seek to enter such tags as evidence, it seems unlikely that courts will jump through each of these hoops to authenticate such a tag on a social networking website because it would take too much time and energy for very little probative value.

Conclusion

Courts are just beginning to shape the law of authenticating social networking websites. Various courts' approaches are shaped by their unfamiliarity with the websites and how they work, which leads to hesitation to fit social networking evidence into the framework of existing authentication procedures for other electronically stored information. Given that hesitation, the trend is for courts to require something beyond typical ESI authentication procedures, including information about the security settings of social networking websites before determining that a given piece of evidence is authentic.[240]

However, as courts become more familiar with social networking websites and their use in court increases, such additional requirements of the "sufficiency" standard may be dropped. Indeed, those additional requirements *should* be dropped—without delay—with respect to messages sent from social networking websites. As described above, there is no difference between sending an electronic communication from an e-mail account or a social networking account. The purpose, function, outbox, privacy settings, and potential for hackers are exactly the same for both types of accounts. Concededly, there may be a need for heightened authentication requirements when it comes to other features of social networking websites, including posts and photographs and especially tags, where the user may not have a record of the communication and where the purpose of the communication may not be clear. But there is simply no need to impose any additional requirements with messages, which lack neither records of sent messages nor clarity of purpose. Thus, the additional requirements should be eliminated for messages as soon as possible, but may remain for some time for other features of social networking websites.

This prediction and recommendation, especially with respect to messages, is not to say that social networking websites will be regularly entered into evidence at trial. Rather, authentication is only the first step for the message, posting, photograph, or other proffered evidence from a social networking website. Like all other types of evidence, even once ESI—including ESI

from social networking websites—makes it past the low threshold of information required for authentication, it is still subject to a number of other evidentiary hurdles, including hearsay,[241] the best evidence rule,[242] Rule 403,[243] Fourth Amendment problems related to how the information was obtained,[244] and—at least in criminal cases when the information is being used against the defendant—the Confrontation Clause. Again, as evidence from social networking websites appears more frequently in the courtroom, courts' approaches to evidentiary issues beyond authentication will become clear, which will affect whether parties actually try to use this type of evidence routinely.

Finally, even when appellate courts find in criminal cases that social networking website evidence was not sufficiently authenticated, the convictions remain intact. This is because courts often find that the admission of unauthenticated messages, postings, or photographs is merely harmless error.[245] Reversible error has been found only when the trial record is replete with the state's references to and repeated reliance on the improperly authenticated evidence throughout the trial and especially during closing argument.[246] Consequently, the fundamental effect of varying the authentication approaches to this type of evidence is unlikely to be a reversal of convictions or judgments.[247] However, trends in the case law will serve to shape the case strategy of parties seeking to admit or exclude this type of evidence. For example, if courts continue to follow the security-driven approach to messages, parties will know that they must bring in an expert to enter the message into evidence.[248] In contrast, if more courts follow the corroboration approach, parties will be forced to focus more on content and surrounding circumstances.[249]

So what does existing case law mean for the courts, for parties, and for users of social networking websites? Courts must be able to adapt to the fast-paced, ever-growing world of the internet. Surely courts cannot reinvent the wheel and create new tests for each different type of internet-produced piece of evidence proffered in every case. Instead, courts must maintain the flexibility intended by Rule 901, seeking to elicit a full picture of the evidence in a way that maintains fairness to all parties. Per the *Griffin* dissent, courts should accept this new category of evidence without hesitation; after all, it will only become more prevalent with time.[250]

Lawyers must come to court expecting a challenge, armed with the knowledge that in all likelihood, litigation is an opportunity to teach the court about social networking websites in a way that benefits their clients. Indeed, most of the cases that deemed proffered evidence inauthentic, provided parties with explicit instructions for next time, identifying for the proponent of the evidence exactly what kind of information would be needed to authenticate the evidence. Most frequently, that information involves experts who can testify to the security settings of social networking websites or digital photography experts who can testify to whether or not a picture has been altered. Given such clear directions by many courts, failure to authenticate social networking evidence in those jurisdictions is truly an avoidable "self-inflicted injury"[251]—provided, of course, that the party can afford to hire such an expert. Case law on this issue will likely evolve over the next few years, albeit at a slower pace than the social networking websites themselves, and advocates must stay up to date on changes in the law while applying it by analogy to whatever new features social networking websites create.

Finally, users of social networking sites must be aware of how their web presences are just a click away from becoming evidence. It would, perhaps, be too much to ask that Facebook, MySpace, and other social networking websites provide *Miranda*-like warnings or disclosure to their users, highlighting the fact that one's online presence can be used against them in a court of law.[252] Indeed, such a request stands in contrast to the purpose of such websites, which foster a forum for sharing information, not limiting it. Yet it is in the websites' best interests to maintain long-term clients, and providing such advice may be perceived as well-intentioned, helpful alerts. Certainly a user would prefer a warning, in lieu of having his own Facebook post used against him at trial.

This type of evidence will likely make its way into the courtroom more frequently over the next few years, as the courts become more familiar with social networking websites and especially as a younger generation of lawyers and clients, constant users of such sites, become parties. Indeed, social networking evidence in the courtroom is already making national headlines in pre-trial proceedings against George Zimmerman, who was charged with second-degree murder of teenager Trayvon Martin in 2012.[253] Because of its publicity, Zimmerman's trial is likely to serve as a touchstone for the use of this type of evidence in criminal trials. Until more jurisdictions, including the Florida county circuit court presiding over George Zimmernan's trial,[254] address these issues head on, parties must be prepared to meet the heightened bar that some courts have set thus far, requiring specific information about security settings and photography technology. While a heightened bar may well be appropriate for posts, tags, and whatever new functions are yet to come to social networking websites, with respect to messages sent from such sites there is simply no need to surpass the sufficiency standard widely used for e-mail evidence today.

---

[1] Julia Mehlman, J.D. 2012, University of California, Berkeley, School of Law, is an associate at Quinn Emanuel Urquhart & Sullivan, LLP in Washington, D.C. Many thanks to Professor Eleanor Swift for her encouragement and advice.

[2] *See, e.g.,* Dina Ely, *10 Brilliant Quotes About Social Media,* INDYPOSTED, (July 20, 2010, 4:16 PM), http://www.indyposted.

com/33903/10-brilliant-quotes-about-social-media/ (quoting Steve Hall of AdGabber, an emerging social media web designer).

[3] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 542 (D. Md. 2007).

[4] *See* Danah Boyd, *Why Youth ¤ Social Network Sites: The Role of Networked Publics in Teenage Social Life*, *in* YOUTH, IDENTITY, AND DIGITAL MEDIA 119, 119 (David Buckingham ed., 2008) (discussing the rising popularity of social networking websites amongst young people).

[5] *See* Emily Nussbaum, *Say Everything*, N.Y. MAGAZINE, Feb. 12, 2007, http://nymag.com/news/features/27341/ (indicating that this generation is more comfortable documenting "what used to be personal information" on social networking websites).

[6] *See* Teddy Wayne, *Age Gap Narrows on Social Networks*, N.Y. TIMES, Dec. 26, 2010, http://www.nytimes.com/2010/12/27/business/media/27drill.html (noting that while just nine percent of internet users between the ages of 55 and 64 used social networks in December, 2008, forty-three percent did so in May, 2010).

[7] This article refers to social networking websites generally, but only examines cases referring to Facebook and MySpace. Certainly, there are other social networking websites in existence, ranging from other general social networking sites like Google+ and Friendster, to dating websites like OKCupid and Match.com, to professional networking sites like LinkedIn and AdGabber. However, this article references only Facebook and MySpace for two reasons: first, these are the websites that have been addressed in case law; and second, these are the websites with which the writer has the most familiarity.

[8] Griffin v. State, 19 A.3d 415, 420 (Md. 2011).

[9] *Id.* at 421 n.9.

[10] Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 845 (W.D. Tex. 2007).

[11] *See id*. at 845-46 (noting the ability of social networking sites to connect its users through an online community of common interests).

[12] *See* Brittany Nay, *Social Networking Use in the Courtroom,* LADUE NEWS (Sept. 20, 2012, 11:12 AM), http://www.laduenews.com/living/business-wealth/social-networking-u...in-the-courtroom/article_05a428d6-033e-11e2-bdc1-001a4bcf6878.html ("Social media is becoming pivotal evidence in a court of law[,]" because of its revealing nature).

[13] 121 AM. JUR. PROOF OF FACTS 3d 1 *Pretrial Involving Facebook, MySpace, LinkedIn, Twitter, and Other Social Networking Tools* § 8 (2011).

[14] *See, e.g.*, Commonwealth v. Williams, 926 N.E.2d 1162, 1171 (Mass. 2010) (noting the use of MySpace computer messages in a criminal murder trial); Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 652 (N.Y. Sup. Ct. 2010) (indicating that the defendant filed a discovery request seeking records from the plaintiff's Facebook and MySpace accounts in a personal injury case).

[15] *See, e.g.*, United States v. Fumo, 639 F. Supp. 2d 544, 555 (E.D. Pa. 2009) (holding that the defendant was not prejudiced by juror's use of Facebook during trial); State v. Dellinger, 696 S.E.2d 38, 40 (W. Va. 2010) (reversing a conviction where a juror was "friends" with the defendant on MySpace); *see also* Bob Egelko, *Jurors to be told not to tweet under new law*, SFGATE (Aug. 6, 2011, 4:00 AM), http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/08/05/BAKM1KK4BM.DTL (discussing a new California state law banning jurors' use of social networking sites and other electronic communications during trial).

[16] *See, e.g.*, Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 568-69 (D. Md. 2007) (stating that the prevalence of social media communications has substantially impacted litigation and evidence collection).

[17] *See, e.g.*, United States v. Nagel, No. CR-10-511, 2011 WL 4025717, at *3 (E.D.N.Y. Sept. 9, 2011) (using MySpace and Facebook messages sent to victims by the defendant as justification for imposing an above-guidelines sentence for a defendant convicted of stalking).

[18] *See, e.g.*, Griffin v. State, 19 A.3d 415, 422-23 (Md. 2011) (asserting that authenticity of electronically stored information is governed by the general rules of authentication, but noting the specific methods of authentication most suitable; *see also* State v. Eleck, 23 A.3d 818, 822-23 (Conn. App. Ct. 2011) (identifying proper methods of authentication for electronically stored information, including witness testimony, expert testimony, and circumstantial facts).

[19] *See, e.g.*, People v. Clevenstine, 891 N.Y.S.2d 511, 514 (N.Y. App. Div. 2009) (admitting MySpace messages into evidence through traditional authentication procedures), *appeal denied*, 925 N.E.2d 937 (N.Y. 2010).

[20] *See Griffin*, 19 A.3d at 424 (rejecting a printout image from a social networking page, noting the potential for abuse due to the ability of someone to manipulate another's social networking site).

[21] *See* FED. R. EVID. 901(a); *see also* Arena v. United States, 226 F.2d 227, 234 (9th Cir. 1955) ("The question of whether the authenticity of a document has been *sufficiently proved* . . . rests in the sound discretion of the trial judge.") (emphasis added), *cert. denied*, 350 U.S. 954 (1956).

[22] *See* Link v. Mercedes-Benz of N. Am., Inc., 788 F.2d 918, 928 (3d Cir. 1986) ("The only requirement is that there has been substantial evidence . . . .").

[23] *Id.*

[24] *See* FED. R. EVID. 901 advisory committee's note to subdivision (a) (stating that authentication denotes relevancy); *see also* R & D Amusement Corp. v. Christianson, 392 N.W.2d 385, 386 (N.D. 1986) ("The purpose of authentication is to establish the document's relevancy.").

[25] *See R & D Amusement Corp.*, 392 N.W.2d at 386 (concluding that a document is properly authenticated when the proponent provides evidence sufficient to show that the document is what the proponent claims it to be).

[26] *See, e.g.*, United States v. Munoz, 16 F.3d 1116, 1120-21 (11th Cir. 1994) (upholding the trial court's authentication of bank documents); United States v. McGlory, 968 F.2d 309, 331 (3d Cir. 1992) (upholding the trial court's authentication of handwritten notes). *But see* United States v. Perlmuter, 693 F.2d 1290, 1292 (9th Cir. 1982) (concluding that the trial court abused its discretion by admitting evidence based on its "aura of authenticity," and not based on federal evidence rules).

[27] FED. R. EVID. 901(a) (emphasis added).

[28] *See, e.g.*, TEX. EVID. R. ANN. 901(a) (West 1998) (using same language as Rule 901); MD. CODE ANN., RULE 5-901 (West 1993) (echoing the language of FRE 901); CAL. EVID. CODE § 403 (West 1965) (separating authentication for writings and non-writings, but requiring substantially similar information as the federal rule).

[29] *See* MCCORMICK ON EVIDENCE, 57-58 (Kenneth S. Broun ed., 6th ed. 2006) (noting that rules of authentication are a necessary check on the perpetration of fraud).

[30] *See id.* at 58 (describing the jury's need for additional contextual background of a writing or document).

[31] *See id.* (citing Mancari v. Frank P. Smith, Inc., 114 F.2d 834 (D.C. Cir. 1940).

[32] *See, e.g.,* First State Bank of Denton v. Md. Cas. Co., 918 F.2d 38, 41 (5th Cir. 1990) (stating that the illustrations provided by the federal rule are not exclusive, all that is necessary is "sufficient authentication to make a *prima facie* case that would allow the issue . . . to be decided by the jury.").

[33] *See* FED. R. EVID. 901(b) (listing different types of evidence that can fulfill the authentication requirement); Fin. Co. of Am. v. BankAmerica Corp., 493 F. Supp. 895, 900 (D. Md. 1980) ("Those methods [of authentication set out in Rule 901], however, are merely illustrations and not limitations upon the manner in which documents may be authenticated.").

[34] *See, e.g.*, FED. R. EVID. 901 advisory committee's note to subdivision (b) ("The examples are not intended as an exclusive enumeration of allowable methods but are meant to guide and suggest, leaving room for growth and development in this area of the law.").

[35] *See* MCCORMICK ON EVIDENCE, *supra* note 29, at 56.

[36] *See, e.g.*, Bazak Int'l Corp. v. Tarrant Apparel Grp., 378 F. Supp. 2d 377, 392 (S.D.N.Y. 2005) (holding that a letter was properly authenticated based on witness testimony).

[37] *See, e.g.*, United States v. Smith, 918 F.2d 1501, 1510 (11th Cir. 1990) (concluding that circumstantial evidence was sufficient to authenticate a ledger). *cert. denied sub nom.*, Hicks v. United States, 502 U.S. 849 (1991).

[38] *See, e.g.*, State v. Swinton, 847 A.2d 921, 945-46 (Conn. 2004) (concluding that witness testimony is an appropriate method to authenticate photographs in light of ongoing technological advances).

[39] *See Smith*, 918 F. 2d at 1510 (noting that circumstantial evidence alone is sometimes sufficient for authentication).

[40] *See* FED. R. EVID. 901 advisory committee's note to subdivision (a) ("[A] telephone conversation may be irrelevant . . . because the speaker is not identified.").

[41] *See id.* (stating that a showing of the author's identity is one of many factors contributing to the authenticity requirement).

[42] *See, e.g.*, United States v. Kassimu, 188 F. App'x. 264, 264 (5th Cir. 2006) (ruling that copies of computer records could be authenticated by a qualified witness with personal knowledge of the procedure that generated the records); Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 545 (D. Md. 2007) (concluding that the authentication requirement for electronically stored information can be met by testimony of either the author or by an expert with specific knowledge about how the information is created and preserved); United States v. Safavian, 435 F. Supp. 2d 36, 40 n.2 (D.D.C. 2006) (noting that e-mail may be authenticated by a witness with personal knowledge of the e-mail's creation).

[43] *See* FED. R. EVID. 901(b) (specifying additional types of evidence other than witness testimony that can satisfy the authentication requirement).

[44] *Id.* at (b)(4).

[45] *See* United States v. Smith, 918 F.2d 1501, 1510 (11th Cir. 1990) (noting the weight of circumstantial evidence for authentication purposes), *cert. denied sub nom.* Hicks v. United States, 502 U.S. 890 (1991).

[46] *See, e.g.,* United States v. McGlory, 968 F.2d 309, 329-331 (3d Cir. 1992) (concluding that the circumstantial evidence offered was sufficient to link the handwritten notes to the defendant).

[47] *Id*.

[48] *See, e.g.*, United States v. Vidacak, 553 F.3d 344, 349 (4th Cir. 2009) (upholding the district court's decision that the Government fulfilled its authentication requirement of military documents through corroborative evidence).

[49] *See* McLain v. Newhouse, 516 F.3d 301, 308 (5th Cir. 2008) (upholding authentication of a ledger sheet); United States v. Dumeisi, 424 F.3d 566, 575 (7th Cir. 2005) (citing United States v. Elkins, 885 F.2d 775 (11th Cir. 1989) "[T]he circumstantial evidence of where the documents were found . . . was sufficient to authenticate the documents in the absence of any evidence of adulteration or forgery."); United States v. Demjanjuk, 367 F.3d 623, 631-32 (6th Cir. 2004) (affirming the district court's authentication of a service pass based on circumstantial evidence); United States v. Tin Yat Chin, 371 F.3d 31, 37 (2d Cir. 2004) (stating that Rule 901 does not "erect a particularly high hurdle," and that circumstantial evidence is sufficient for authentication); United States v. Holmquist, 36 F.3d 154, 169 (1st Cir. 1994) (concluding that a photograph can be properly authenticated by direct or circumstantial evidence, without the need for witness testimony); United States v. Hernandez-Herrera, 952 F.2d 342, 344 (10th Cir. 1991) (authenticating a fingerprint card based on circumstantial evidence); United States v. Elkins, 885 F.2d 775, 785 (11th Cir. 1989); United States v. Eisenberg, 807 F.2d 1446, 1452 (8th Cir. 1986) (noting that the content and appearance of a document can serve as evidence to authenticate it); Alexander Dawson, Inc. v. N.L.R.B., 586 F.2d 1300, 1302 (9th Cir. 1978) (concluding that direct or circumstantial evidence can authenticate a document); United States v. Sutton, 426 F.2d 1202, 1207-08 (D.C. Cir. 1969) (stating that authorship of a document for authentication purposes can be shown through circumstantial evidence, such as personal information in the document only known to the purported author).

[50] *See, e.g.*, Bodrey v. Bodrey, 269 S.E.2d 14, 15 (Ga. 1980) (noting that authorship of a love letter found by the appellant's wife was immaterial; instead proof of relevancy was required, which was satisfied by the fact that the wife *found* the letter) (emphasis added).

[51] *See, e.g.*, *id.* (noting that the relevance of whether appellant's wife found a love letter was not whether the letter was true, but to explain the wife's subsequent conduct).

[52] *See, e.g,* FED. R. EVID. 901(b)(1) (permitting testimony by a witness with knowledge).

[53] *See* FED. R. EVID. 901(b) (noting that the illustrations, including witness testimony, are merely examples and not a complete list of evidence that can satisfy the authentication requirement).

[54] *See* United States v. Reilly*,* 33 F.3d 1396, 1404 (3d Cir. 1994) (noting that the connection between a message and its source may be established by circumstantial evidence); United States v. Clark, 649 F.2d 534 (7th Cir. 1981) (holding that circumstantial evidence is sufficient to establish authenticity of a document).

[55] *See, e.g.*, United States v. Tank, 200 F.3d 627, 630-31 (9th Cir. 2000) (holding that the chat room log printouts were adequately authenticated when the defendant showed up to a meeting arranged through the chat room).

[56] *See id*. (upholding the authentication of a chat room log printout because of sufficient circumstantial evidence linking the appellant to the chat room).

[57] *See* United States v. Brewer, 630 F.2d 795, 802 (10th Cir. 1980) (discussing the court's responsibility to decide whether "there is a reasonable probability that the evidence has not been altered in any material aspect since the time of the crime.").

[58] *See* People v. Beckley, 110 Cal. Rptr. 3d 362, 366 (Ct. App. 2010) (noting the heightened untrustworthiness of photographs as evidence due to the ease with which they can be digitally manipulated), *as modified on denial of reh'g* (June 24, 2010), *review denied* (Sept. 22, 2010), *cert. denied sub nom.* Beckley v. California, 131 S.Ct. 1522 (2011).

[59] *See* United States v. Stearns, 550 F.2d 1167, 1170 (9th Cir. 1977) (stating that a photograph may be inadmissible due to its distortion or manipulation, or because the scene portrayed in the photograph is irrelevant).

[60] *Id.*

[61] *See id*. (noting the importance of the photographs' relevancy for authentication purposes).

[62] *See id.*

[63] *See generally* United States v. Seifert, 445 F.3d 1043, 1044 (8th Cir. 2006) (upholding the district court's decision to admit video surveillance even though it was digitally-enhanced and therefore altered from its original state).

[64] *See, e.g.*, *id.* at 1045 (noting that enhancement of a surveillance tape did not alter its imagery); *see also* United States v. Beeler, 62 F. Supp. 2d 136, 149 (D. Me. 1999) (noting that a witness testified to editing and enhancing the quality of a video tape without modifying its content).

[65] *See Seifert*, 445 F.3d at 1045 (affirming appellant's arson conviction based largely on incriminating surveillance video which was altered for use at trial).

[66] *See id*. (noting that the original surveillance video was "time lapsed").

[67] *See id*.

[68] *Id*.

[69] *See Beeler*, 62 F. Supp. 2d at 148 (rejecting the defendant's argument that copies of surveillance video should be inadmissible because they have been modified through digital enhancement).

[70] *See id.* at 149 (noting that the images from the video were shaded for better visibility, but not altered in their content).

[71] *Id.* at 149-50.

[72] *See* United States v. Frabizio, 463 F. Supp. 2d 111, 112-13 (D. Mass. 2006) ("Photoshop and other, similar programs . . . suggest[] it may be possible to digitally create or manipulate photographs in a manner the naked eye cannot detect.")

[73] *See, e.g.*, United States v. Berringer, 601 F. Supp. 2d 976, 977-79 (N.D. Ohio 2008) (discussing the use of technology in "virtual child pornography" in which minors appear to engage in sexually explicit images but were added into the scene using computer imaging technology).

[74] See Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 542-43 (D. Md. 2007) (acknowledging that higher standards for authenticity may be required, but that it is unnecessary to completely abandon the use of traditional evidence rules).

[75] *See id.* at 541- 42 (examining cases from the First, Third, Fourth, Fifth, Seventh, Ninth, Tenth, Eleventh Circuits, and several district courts).

[76] *Id*. at 538.

[77] *Id*. at 543.

[78] *See* Catherine Guthrie & Brittan Mitchell, *The Swinton Six: The Impact of State v. Swinton on the Authentication of Digital Image*,, 36 Stetson L. Rev. 661, 664-65 (2007) (detailing alterations available for digital images, including reparative and visual enhancement techniques).

[79] *See, e.g.*, St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d. 773, 775 (S.D. Tex. 1999) (requiring the plaintiff to present hard copy documentation instead of arbitrary information found on the internet to support plaintiff's argument).

[80] McCormick on Evidence, *supra* note 29, at 74.

[81] *See id.* at 72-73 (noting courts' flexibility regarding the admissibility of electronic technologies such as emails and web postings).

[82] *See id.* at 72-73.

[83] *See, e.g.*, People v. Clevenstine, 891 N.Y.S.2d 511, 513 (N.Y. App. Div. 2009) (MySpace messages); State v. Eleck, 23 A.3d 818, 822 (Conn. App. Ct. 2011) (Facebook and MySpace messages); Griffin v. State, 19 A.3d 415, 426 (Md. 2011) (Facebook wall posts); People v. Beckley, 110 Cal. Rptr. 3d 362, 363 (Ct. App. 2010) (MySpace photograph); People v. Lenihan, 911 N.Y.S.2d 588, 591 (N.Y. Sup. Ct. 2010) (same).

[84] *See* Linda Listrom et. al, *The Next Frontier: Admissibility of Electronic Evidence*, 1, at 9, *available at* http://www.mccarthyfingar.com/files/20110129123145-A%20B%20A%20(00276545).PDF (noting that testimony of a witness with direct knowledge about a web posting is sufficient evidence for its authentication).

[85] *See, e.g.*, *Clevenstine*, 891 N.Y.S.2d at 513 (in rape case in which prosecution sought to offer a MySpace message allegedly sent by the defendant, defendant did not testify); *Eleck*, 23 A.3d at 821 (witness who allegedly sent Facbeook messages testified that the account was hers but denied writing or sending the messages at issue).

[86] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 553 (D. Md. 2007).

[87] *See, e.g.*, State v. Eleck, 23 A.3d 818, 822 (Conn. App. Ct. 2011) (relating e-mails and text messages to Facebook and MySpace messages because each of these forms of communication could be "generated by someone other than the named sender"); *see also* People v. Clevenstine, 891 N.Y.S.2d 511, 513 (N.Y. App. Div. 2009) (noting the defendant's argument that someone else sent incriminating MySpace messages from his account), *appeal denied*, 925 N.E.2d 937 (N.Y. 2010).

[88] *Lorraine*, 241 F.R.D. at 555.

[89] *See id.* at 556 (specifying methods available for authenticating website postings).

[90] *See id*. at 554-55 (concluding that the sender address alone is not sufficient evidence to authenticate an e-mail); *Clevenstine*, 891 N.Y.S.2d at 513 (requiring witness testimony in addition to a sender address to authenticate MySpace messages).

[91] *See Clevenstine,* 891 N.Y.S.2d at 513 (the "email parallel approach"); Manuel v. State, 357 S.W.3d 66, 75 (Tex. Ct. App. 2011) (the "corroboration approach"); *Eleck*, 23 A.3d at 822 (the "security approach").

[92] *See Clevenstine*, 891 N.Y.S.2d at 514 (likening MySpace messages to emails and requiring no extra information for authentication).

[93] *See Manuel*, 357 S.W.3d at 75 (requiring corroborating evidence of unique content to authenticate MySpace messages); Commonwealth v. Williams, 926 N.E.2d 1162, 1172 (Mass. 2010) (requiring corroborating evidence of authorship to authenticate MySpace messages)

[94] *See Williams*, 926 N.E.2d at 1171 (Mass. 2010) (highlighting the need for evidence about MySpace's security settings); *State v. Eleck*, 23 A.3d 818, 822 (Conn. App. Ct. 2011) (same).

[95] *See, e.g.*, *Eleck*, 23 A.3d at 822 (Conn. App. Ct. 2011) (requiring both corroborating evidence of authorship and additional evidence about Facebook's security settings).

[96] *See Clevenstine*, 891 N.Y.S.2d at 514 (rejecting defendant's argument that someone else could have accessed his MySpace account and sent the messages, leaving the issue for the jury).

[97] *See id*. at 513.

[98] *See id*.

[99] *See id.* at 514.

[100] *See id.*

[101] *Clevenstine*, 891 N.Y.S.2d at 514 (explaining that the defendant's argument went to the weight of the evidence and not to the admissibility of the evidence).

[102] *See id.*, (rejecting the defendant's argument that insufficient evidence was presented to authenticate the messages).

[103] *See id.* (finding the messages properly authenticated and noting that the defendant's arguments against authentication go to the evidence's weight rather than admissibility).

[104] *See id.*

[105] *See, e.g.*, Commonwealth v. Williams, 926 N.E.2d 1162, 1172 (Mass. 2010) (excluding the admissibility of MySpace messages sent from the defendant's account because insufficient proof existed to conclude that the messages had been generated and sent by the defendant himself); *see also* State v. Eleck, 23 A.3d 818, 822 (Conn. App. Ct. 2011) (noting the possibility that someone can access another person's private e-mail or Facebook account).

[106] *See Eleck,* 23 A.3d at 822 (stating that the Facebook messages had not been sufficiently authenticated, and required either forensic computer evidence or corroborative facts to do so).

[107] *See, e.g.*, United States v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (finding e-mails to be authenticated based on the e-mail address and factual details known only to the defendant that were corroborated by later telephone conversations);.United States v. Tank, 200 F.3d 627, 630-31 (9th Cir. 2000) (finding the author of chat room messages identified for authentication purposes when the author showed up at a meeting arranged during the chat session); *see also* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 546 (D. Md. 2007) (noting the authentication of instant message transcripts based on witness testimony that corroborated other circumstantial evidence).

[108] *See, e.g.*, United States v. Kassimu, 188 F. App'x. 264, 264 (5th Cir. 2006) (holding that postal records were properly authenticated based on corroborative expert testimony); *Siddiqui*, 235 F.3d at 1322 (using the corroboration approach in the Eleventh Circuit); *Lorraine,* 241 F.R.D. at 546 (noting that circumstantial and direct facts are needed for authentication of a document); United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (stating that identifying the sender address of an email is not sufficient evidence to prove authorship of an email).

[109] *See, e.g.*, Manuel v. State, 357 S.W.3d 66, 75 (Tex. Ct. App. 2011) (noting that text messages, instant messages, MySpace evidence, and Facebook messages, can be authenticated by using the same factors to authenticate e-mails based on the "'[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics taken in conjunction with circumstances.'").

[110] *See id*. at 69 (stating that the appellant utilized electronic communications as a method of threatening the victim).

[111] *See id.* at 75 (citing Massimo v. State, 144 S.W.3d 210, 215-17 (Tex. Crim. App. 2004) in considering an email message's substantive and distinctive characteristics along with the circumstances of its delivery).

[112] *See id*. at 81.

[113] *See id.* at 79 (noting corroborative facts that authenticated the electronic communications sent from the defendant to his stalking victim).

[114] *See, e.g.*, United States v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (authenticating e-mails not only by use of the defendant's e-mail address, but by inclusion of factual details known only to the defendant that were corroborated by telephone conversations); United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (authenticating e-mails not only by use of the defendant's e-mail address, but by inclusion of content known only to the defendant, use of the defendant's nickname, and testimony by witnesses that the defendant spoke to them about the subjects contained in the e-mail).

[115] *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 546 (D. Md. 2007) (citing to Federal Rule 901(b)(4) in reference to the "circumstantial evidence rule" of authentication).

[116] *See, e.g.*, State v. Eleck, 23 A.3d 818, 822 (Conn. App. Ct. 2011) (noting the potential for manipulation or abuse to one's social media account by another and thus, requiring more than showing whose account a message came from for authentication).

[117] *See id.* at 820 (rejecting the defendant's claim that the lower court erred when it barred from evidence a Facebook message sent from the victim's account to the defendant's account).

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] *See id.* (stating that the victim said she only saw the defendant in public and never exchanged any type of communications with him).

[122] *See id.* at 820-21.

[123] *See Eleck*, 23 A.3d at 821.

[124] *See id.* at 820.

[125] *See id*.

[126] *See id.* (clarifying that the hacker had changed the password to her account after the messages were sent from her account, suggesting that she still had access at the time the messages were sent).

[127] *See id.* at 821 (sustaining the lower court's holding that the messages were not properly authenticated because the victim's authorship was not sufficiently shown).

[128] *Eleck*, 23 A.3d. at 822 ("[p]roving only that a message came from a particular account, without further authenticating evidence, has been held to be inadequate proof of authorship.").

[129] *See id.* at 821.

[130] *See id*. at 824 (upholding the trial court's ruling that the defendant failed to present sufficient corroborative facts for authentication of the Facebook messages).

[131] *See id.* at 823 (identifying ways to corroborate telephone conversations, letters on a computer hard drive, and electronic messaging).

[132] *See id.* (suggesting that the proponent of the evidence investigate the search history of the alleged author's computer to prove authorship of an electronic message).

[133] *Eleck*, 23 A.3d. (noting that the purported author's writing style or personal references can serve as corroborative evidence to prove authorship of letters on a hard drive).

[134] *Id.* at 824.

[135] *See id.* at 824 (agreeing with the lower court that the subject matter of the conversation was not peculiar enough to implicate the defendant as the only possible sender).

[136] *See id.* at 823 (reasoning that in operating a computer the user inadvertently leaves an evidential trail for someone with the knowhow to find, providing evidence of their internet usage).

[137] *See United States v. Kennedy*, 81 F. Supp. 2d 1103, 1105 n.3 (D. Kan. 2000) ("The IP, or Internet Protocol, address is unique to a specific computer. Only one computer would be assigned a particular IP address.").

[138] However, even showing that the account was accessed from a given computer based on IP address information does not foreclose the possibility that an unauthorized user logged into the witness' computer in order to hack the account.

[139] *See Eleck*, 23 A.3d. at 824 (finding that the reply "the past is the past" in response to the defendant's inquiry regarding why the witness was speaking to him contained no information that was specific to or only known by the witness).

[140] *See id.*

[141] *Compare Eleck*, 23 A.3d. at 825 (requiring security testimony in conjunction with corroborative evidence), *with* People v. Clevenstine, 891 N.Y.S.2d 511, 514 (N.Y. App. Div. 2009) (requiring only corroborative testimony), *appeal denied*, 925 N.E.2d 937 (N.Y. 2010).

[142] *Eleck*, 23 A.3d. at 824.

[143] Fed. R. Evid. 403.

[144] *See Eleck*, 23 A.3d. at 822 (discussing the relative ease with which one can masquerade under another person's name on a social networking site by either creating a fake profile or gaining access to a person's actual account by cracking their username and password, or by simply gaining access to an unattended electronic device that is still logged on to a personal site).

[145] *See* Griffin v. State, 19 A.3d 415, 424-25 (Md. 2011); *see also* Commonwealth v. Williams, 926 N.E.2d 1162, 1172 (Mass. 2010) (requiring testimony that the defendant's brother was the only one who could communicate from his MySpace page).

[146] *See Williams,* 926 N.E.2d at 1172 (comparing a MySpace Web page to a telephone call, the court held that testimony from a witness claiming to receive a message from another, without anything more, is not enough to authenticate the message).

[147] *See id.* at 1171. (denying defendant's motion to strike the witness' testimony, but refusing to admit a printout of the messages).

[148] *See id*. at 1172 (holding that the foundational testimony did not identify the actual sender, since no testimony was proffered as to how secure a MySpace Web page is).

[149] *Id*. at 1172.

[150] *See Griffin*, 19 A.3d at 427-28 (requiring a greater degree of authenticity than what was established by the evidence provided, noting that the particular evidence or testimony may have changed the outcome of the case); *see also* State v. Eleck, 23 A.3d 818, 820-21 (Conn. App. Ct. 2011) (requiring testimony on security protocols before allowing the defendant to impeach the state's witness).

[151] *See* People v. Clevenstine, 891 N.Y.S.2d 511, 513-14 (N.Y. App. Div. 2009) (upholding the defendant's conviction and explaining that the overall weight of the evidence, including testimony of the victims that included specific dates and details of the sexual intercourse along with corroboration by the defendant's wife, overshadowed the importance of the MySpace conversations), *appeal denied*, 925 N.E.2d 937 (N.Y. 2010).

[152] *See id.* (holding that, in light of the facts surrounding the case, the possibility that someone else other than the defendant sent the message was a question of fact for the jury rather than an issue of authentication).

[153] *See Eleck*, 23 A.3d. at 820 (requiring heightened authentication requirements, such as testimony about security protocols).

[154] *See, e.g.*, *id.* (establishing a higher bar for authentication of messages from social networking websites compared to emails because of the websites' security weaknesses without explaining the security differences between social networking websites and email platforms).

[155] *See, e.g.*, *id.* at 820-21 (noting a heightened concern for hacking of social networking accounts compared to email accounts without providing any explanation); Griffin v. State, 19 A.3d 415, 426 (Md. 2011) (same).

[156] *See* Kathrine Minotti, Note, *The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession*, 60 S.C. L. Rev. 1057, 1064-65 (2009) (arguing that both email and Facebook messages are structurally and functionally similar; they both go to inboxes, the inboxes are password protected, and the communication itself is facilitated by a third party).

[157] *See Eleck*, 23 A.3d. at 822 (combining the corroboration and security approaches raises the bar that one has to clear to authenticate social networking evidence; even if one can prove that a message came from a certain account, the proponent must also prove it that the account was used by its purported user).

[158] *Cf.* Brian Krebs, *Hackers' Latest Target: Social Networking Sites*, Wash. Post, Aug. 9, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/08/08/AR2008080803671.html (reporting that as a result of the plethora of ways to hijack accounts, social networking sites have become "the most fertile grounds for… identity thieves and online mischief makers"); *see also* Gary LosHuertos, *Herding Firesheep in Starbucks*, CNNMoney (Dec. 16, 2010, 1:48 PM) http://money.cnn.com/2010/12/14/technology/firesheep_starbucks/index.htm (demonstrating how a simple web application allowed the author to quickly and effortlessly collect Facebook and Twitter accounts from users in Starbucks, and then send those same users messages from their own accounts).

[159] *See* Scott Charles Silverman, Creating Community Online: The Effect of Social Networking Communities on College Students' Experiences 55 (Dec. 2007) (unpublished Ph.D dissertation, on file with Rossier School of Education, University of Southern California) (discussing the frequency with which "fakesters" create accounts in other people's names).

[160] *Cf.* Commonwealth v. Williams, 926 N.E.2d 1162, 1173 (Mass. 2010) (excluding testimony regarding the content of MySpace messages because there was no testimony regarding security settings).

[161] *See Eleck*, 23 A.3d. at 822 (noting that electronic communication is particularly vulnerable to the possibility that the named sender did not actually generate the message due to the presence of hackers, and through the negligence of the user who remains logged in while leaving his or her computer or cell phone unattended).

[162] State v. Eleck, 30 A.3d 2 (Conn. 2011) (granting *certiorari* to determine whether "the Appellate Court properly determine[d] that the trial court did not abuse its discretion in concluding that Facebook messages purportedly sent by a witness were inadmissible because they lacked sufficient authentication[.]").

[163] *See, e.g.*, Griffin v. State, 19 A.3d 415, 426 n.13 (Md. 2011) (noting, and providing examples, that unlike an email, which is only intended for the eyes of the specified recipient, a Facebook or MySpace wall post is open for the world at large to see).

[164] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 n. 4 (D. Md. 2007).

[165] *See id.* at 555 (refusing to "require proof that the [online] postings had been done by the defendant or with [his] authority, or evidence to disprove the possibility that the contents had been altered by third parties."); *but see* St. Clair v. Johnny's Oyster and Shrimp, Inc., 76 F.Supp.2d 773 (S.D.Tex.1999) (stating that evidence procured from online sources is "voodoo information" and that the internet is "one large catalyst for rumor, innuendo, and misinformation").

[166] Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980 (C.D. Cal 2010).

[167] *Id.* at 981 (emphasis removed).

[168] *Griffin,* 19 A.3d at 420.

[169] *See* Megan Uncel, Comment, "*Facebook is Now Friends With the Court": Current Federal Rules and Social Media Evidence,* 52 Jurimetrics J. 43, 79-83 (2011) (explaining that there are no hard statistics about the frequency of fake profiles. Registration for the majority of social-networking sites is free and asks only for the bare minimum of personal information, which makes it difficult to verify the identity of the person behind the profile).

[170] *See Griffin,* 19 A.3d at 418.

[171] *See id.* at 417.

[172] *See id.* at 418 (describing that most of the print outs of the profile page were redacted, and the only portion not redacted contained the threat at issue in the case).

[173] *See id*. at 418.

[174] *See id.*

[175] *Griffin,* 19 A.3d at 418.

[176] *See id.*

[177] *See id*. at 418.

[178] *See id*. at 419 (acknowledging that the defense counsel agreed to this stipulation in lieu of Sergeant Cook's testimony, although the defense still maintained their objection to the admittance of the evidence).

[179] *See id.*

[180] *Griffin,* 19 A.3d at 419.

[181] *See id.* at 420 (noting that many social networking sites, like MySpace, allow members to create online profiles at no cost as long as they have an email address and purport that they are over the age of fourteen).

[182] *See id.* (quoting Nathan Petrashek, Comment, *The Fourth Amendment and the Brave New World of Online Social Networking*, 93 Marq. L. Rev. 1495, 1499-1500 (2009-2010)); *see also* Silverman, *supra* note 159, at 55 (discussing the possibility that a user is viewing either a fake profile or a real profile that does not reflect the true persona of the person posting the information).

[183] *See id*. at 420.

[184] *Id*. at 421.

[185] *Griffin,* 19 A.3d at 422.

[186] *See id*. at 422-23 (relying on the discussion in Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. Md. 2007).

[187] *See id*. at 424.

[188] *See id.* at 424 (recognizing that greater scrutiny is required because of the inherent anonymity of internet users, and the importance of discovering who the underlying author is).

[189] *See id.* at 427-28.

[190] *See Griffin,* 19 A.3d at 423 (finding that the State did not sufficiently authenticate the evidence by failing to offer any extrinsic evidence describing MySpace or how the investigator obtained the pages).

[191] *See id.* at 419.

[192] *See id*. at 418 (reversing the lower court in a 5-2 decision).

[193] *See id*. at 424, n. 12 & 430 (inferring that the majority was too concerned about the potential for manipulation and that the issue should have gone to the trier of fact).

[194] *See id.* at 429 (Harrell, J., dissenting) (reasoning that a picture of someone who looks like the witness posing with the witness's boyfriend, a birthday matching the witness's, a short description about the purported creator of the page that matches the witness, and references to freeing "Boozy"–the nickname of the defendant—was enough to convince a reasonable jury that the MySpace page is what the State purported it to be).

[195] *Griffin,* 19 A.3d at 430 (Harrell, J., dissenting).

[196] *See id.* (Harrell, J., dissenting) (reasoning that if a reasonable juror can conclude that the evidence is what it purports to be, then it should be admitted).

[197] *See id.* at 422 (recognizing the relative ease with which anyone can create fictional personas or gain unauthorized access to another user's profile).

[198] *See id.* at 423. Likewise, in the context of messages, the risk of hackers was allocated to the proponent in *Eleck*. In that case, the proponent had to offer corroborating evidence that effectively minimized the likelihood

that the account had been hacked in order to meet the sufficiency standard. *See* State v. Eleck, 23 A.3d 818, 820-22 (Conn. App. Ct. 2011) (requiring extrinsic evidence that the witness authored the messages).

[199] *See* Allison L. Pannozzo, Note, *Uploading Guilt: Adding a Virtual Records Exception to the Federal Rules of Evidence,* 44 Conn. L. Rev. 1693, 1701 (2012) (explaining that while the content of social media can be relevant, the ease with which one can post whatever they are thinking at any precise moment often leads to false statements or exaggerations that have a great chance of unfairly prejudicing a jury).

[200] *See Griffin,* 19 A.3d at 427 (stating that the State sought to introduce the content of Ms. Barber's statement for the truth of the matter asserted: that she had threatened a key witness).

[201] *See id*. (referring to the post which stated, "FREE BOOZY!!! JUST REMEMBER SNITCHES GET STICHES!! U KNOW WHO YOU ARE!!").

[202] *About Social Networking*, Staying Safe Online, Jan. 26, 2008, http://www.stayingsafeonline.com/Social%20Networking.htm (suggesting that in the absence of face-to-face contact, people can become bolder); *see also* J. Preece & Diane Maloney-Krichmar, *Online Communities: Focusing on sociability and usability*, *in* Handbook of Human-Computer Interaction 596, 605 (J. Jacko & A. Sears, eds., 2003) (explaining that people who lack self confidence in face to face interactions become more confident online and lose their inhibitions, knowing that they have the ability to turn off the computer).

[203] *See* Silverman, *supra* note 159, at 55 (describing "fakesters" that pretend to be someone else).

[204] Michelle Sherman, *The Anatomy of a Trial with Social Media and the Internet,* 14 J. Internet L. 11, 13 (2011).

[205] Facebook.com, "Report This Photo,", http://www.facebook.com/photo.php?fbid=10101310379450928&set=a.10100240756444008.2712801.5707091&type=1&theater (last visited Oct. 1, 2012).

[206] *See* People v. Beckley, 110 Cal. Rptr. 3d 362, 363 (Ct. App. 2010) (addressing MySpace photograph), *as modified on denial of reh'g* (June 24, 2010), *review denied* (Sept. 22, 2010), *cert. denied sub nom.* Beckley v. California, 131 S.Ct. 1522 (2011); People v. Lenihan, 911 N.Y.S.2d 588, 591 (N.Y. Sup. Ct. 2010) (addressing a MySpace photograph).

[207] *See Beckley*, 110 Cal. Rptr. 3d at 366; *Lenihan*, 911 N.Y.S.2d at 592 (describing two ways to authenticate a photograph: (1) by personal observation or (2) by expert testimony).

[208] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 561 (D. Md. 2007).

[209] *Id*. at 561.

[210] *See id*.

[211] *See id.* at 561-62 (explaining that, in the case of photographs, there are three distinct types in regards to authentication: original digital images, digitally converted images and digitally enhanced images. A MySpace image will typically be found in the original digital image category. In that case, the proponent of the image must find a witness who had personal knowledge of the scene depicted. If there is any question about the picture's reliability, it would behoove the proponent to produce an expert witness to testify about the lack of tampering).

[212] *See Beckley*, 110 Cal. Rptr. 3d at 364 (holding unanimously that photographs downloaded from MySpace were not properly authenticated because the officer who obtained the photographs could not testify from his personal knowledge that the photograph represented what he claimed it did, nor was there an expert who could testify to prove the picture was not impermissibly altered).

[213] *See id.* at 365 (summarizing the evidence that in April, 2007, two gangs scuffled multiple times, which resulted in a May, 2007 drive-by shooting. Beckley argued that he was no longer part of the gang. In response, the prosecution attempted to admit evidence of gang activity recovered from Beckley's MySpace page).

[214] *See id*.

[215] *See id*.

[216] *See id.* at 366 (arguing that the photograph could have been a composite of the defendant's face and someone else's body).

[217] *Beckley*, 110 Cal. Rptr. 3d at 366 (quoting Cal. Evid. Code §§ 250, 1401, and reviewing cases where photographs were treated as writings for authentication purposes).

[218] *Id.* at 367.

[219] *See id.* (recognizing the generally skeptical attitude courts hold regarding evidence obtained from the internet).

[220] *See id.* at 366 (upholding admission of a photograph of defendants committing the crime where a photographic expert testified that the picture was not a composite and had not been faked).

[221] *See* Theodore J. Greeley, *The Plight of Indigent Defendants in a Computer-Based Age: Maintaining The Adversarial System By Granting Indigent Defendants Access to Computer Experts,* 16 Va. J.L. & Tech 400, 410 (2011) (explaining that despite the Criminal Justice Act, which provides limited funding for indigent defendants in federal courts, many defendants do not get the experts they need because of the Court's unwillingness to exercise their power to appoint experts, their lawyer's lack of training and resources to obtain experts, and the significant limitations on the power of courts to appoint experts. Costs over $2,400 must be approved by the chief judge of the circuit, and the services must be "necessary to provide fair compensation for services of an unusual character or duration.").

[222] *See Beckley*, 110 Cal. Rptr. 3d at 367.

[223] *See id*. (reasoning that it was not likely that Beckley would have been acquitted of the charges even if the court did not admit the photograph).

[224] *See* People v. Lenihan, 911 N.Y.S.2d 588, 592 (N.Y. Sup. Ct. 2010) (holding that the ability to "photo shop" a digital photograph precluded the photograph from being authenticated).

[225] *See id.* (explaining the defendant's argument that the prosecution's witnesses were in a gang together, and thus had a motive to fabricate a story that implicated the defendant, who they may have thought was in a rival gang).

[226] *See id.* at 592 (noting that defendant's theory for the witness' motive was too remote and speculative).

[227] *See id.* at 591.

[228] *Id.* at 592.

[229] *See Lenihan*, 911 N.Y.S.2d (holding that, by themselves, the clothing and certain hand gestures of the witnesses in the photographs did not provide a good faith basis to permit the defendant to cross-examine them about gang affiliation).

[230] *See id.* at 592-93.

[231] *See, e.g.*, Amy Clark, *Employers Look at Facebook, Too*, CBS News, (Feb. 11, 2009 6:21 PM), http://www.cbsnews.com/stories/2006/06/20/eveningnews/main1734920.shtml (warning college students not to post photographs from social events).

[232] *See* People v. Beckley, 110 Cal. Rptr. 3d 362, 366 (Ct. App. 2010), *as modified on denial of reh'g* (June 24, 2010), *review denied* (Sept. 22, 2010), *cert. denied sub nom.* Beckley v. California, 131 S.Ct. 1522 (2011).

[233] *See id.* at 364 (finding that the MySpace photograph was impermissibly admitted without expert testimony establishing the veracity of the photographs); *Lenihan,* 911 N.Y.S.2d at 592 (holding that the lower court was justified in precluding the use of a MySpace photograph absent expert verification of non-tampering).

[234] *See Beckley*, 110 Cal. Rptr. 3d at 366; *Lenihan*, 911 N.Y.S.2d at 592 (suggesting that the proponent of the photograph should either find a witness who was present at the time the picture was captured or have an expert testify about its authenticity).

[235] *See Beckley*, 110 Cal. Rptr. 3d at 366 (holding that the photograph was not properly authenticated because the officer could not testify from his personal experience that the photograph was not fabricated; instead, expert testimony was needed to authenticate the images).

[236] Evan E. North, Comment, *Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites*, 58 U. Kan. L. Rev. 1279, 1290 (2010).

[237] *See id.* at 1304.

[238] *Id*.

[239] *See* Paul Boutin, *12 Things You Didn't Know Facebook Could Do*, N.Y. Times, Nov. 30, 2011, http://www.nytimes.com/2011/12/01/technology/personaltech/12-things-you-didnt-know-facebook-could-do.html?scp=8&sq=facebook%20photos&st=cse.

[240] *See, e.g.*, Daniel K. Gelb & Richard M. Gelb, *Electronic Discovery in Criminal Litigation and Regulatory Proceedings,* Mass. CLE, Inc. § 5.7 (2011) (stating that text, audio, or video found on a social-media sites does not make the evidence per se admissible).

[241] *See, e.g.*, Novak v. Tucows, Inc., No. 06-CV-1909(JFB), 2007 WL 922306, *1 (E.D.N.Y. Mar. 26, 2007) ("Where postings from internet websites are not statements made by declarants testifying at trial and are offered to prove the truth of the matter asserted, such postings generally constitute hearsay under Fed. R. Evid. 801.").

[242] *See, e.g.*, Commonwealth v. Amaral, 941 N.E.2d 1143, 1147 (Mass. App. Ct. 2011) (addressing and rejecting the defendant's objection to admitting printed copies of communications pursuant to the 'Best Evidence Rule').

[243] *See, e.g.,* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538 (D. Md. 2007) (addressing whether "the probative value of the ESI [is] substantially outweighed by the danger of unfair prejudice or one of the other factors identified by rule 403, such that it should be excluded despite its relevance.").

[244] *See, e.g.,* Nathan Petrashek, *supra* note 182 at 1513-1531 (addressing Fourth Amendment issues as they relate to the internet, including expectation of privacy, search and seizure, and the public vantage doctrine).

[245] *See, e.g.*, People v. Beckley, 110 Cal. Rptr. 3d 362, 364 (Ct. App. 2010) (noting that the error was harmless because the wrongfully admitted evidence was cumulative and there was copious alternative evidence to prove the defendant's membership in the gang), *as modified on denial of reh'g* (June 24, 2010), *review denied* (Sept. 22, 2010), *cert. denied sub nom.* Beckley v. California, 131 S.Ct. 1522 (2011).

[246] *See, e.g.*, Griffin v. State, 19 A.3d 415, 427 (Md. 2011) (holding that the MySpace printout that contained the threat "snitches get stiches" was a key component in the prosecution's case, and the lower court's error in admitting it requires a reversal of the disposition).

[247] *See, e.g.*, State v. Eleck, 23 A.3d 818, 825 (Conn. App. Ct. 2011) (citing a line of cases regarding authentication of ESI; each one referred to a different level of circumstantial evidence required to admit ESI into evidence).

[248] *See, e.g.*, Breanne M. Democko, Comment, *Social Media and the Rules on Authentication,* 43 U. Tol. L. Rev. 367 (2012) (discussing Commonwealth v. Williams, 926 N.E.2d 1162 (Mass. 2010), where the court noted the lack of expert testimony to verify that no one other than the defendant could communicate from the defendant's profile).

[249] *See, e.g.*, John G. Browning, *Digging for the Digital Dirt: Discovery and the Use of Evidence from Social Media Sites,* 14 SMU Sci. & Tech. L. Rev. 465, 479 (2011) (examining a line of cases that found social media evidence authenticated based on confirmation of screen names and corroboration of sent messages through actions by the defendant).

[250] *See Griffin*, 19 A.3d at 429-30 (Harrell, J., dissenting) (arguing that despite the majority's "technological heebie jeebies," the court should apply the "reasonable juror" standard to electronic evidence); Democko, *supra* note 248, at 311 (discussing that while technology is constantly evolving, the rules regarding authentication are flexible; specifically, "Rule 102 further instructs courts to interpret the rules in order to 'promot[e]. . . growth and development in the law of evidence.'").

[251] *See, e.g.*, Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 542 (D. Md. 2007) 452 (discussing federal and state cases across jurisdictions where ESI evidence was rejected by the court due only to a failure to properly authenticate it).

[252] *See, e.g.*, Peter Kozinets & Aaron J. Lockwood, *Discovery in the Age of Facebook,* 47 Ariz. Att'y 42, TBA (2011) (noting that "social media already has been used in a wide range of litigation." Individuals' online presence may be used against them in other areas as well, as employers have begun to investigate the social media presence of applicants).

[253] Lizette Alvarez, *Judge Rules Trayvon Martin Files Can Be Used By Defense*, N.Y. Times, Oct. 19, 2012, http://www.nytimes.com/2012/10/20/us/judge-in-trayvon-martin-case-says-his-files-can-be-used.html ("The judge . . . said Mr. Martin's Twitter, Facebook, and school records were relevant in the self-defense case.").

[254] *See* Zimmerman v. State, No. 5D12-3198, 2012 WL 3758666 (Fla. Dist. Ct. App. Aug. 29, 2012).

About the Author

Julia Mehlman earned her Juris Doctorate from the University of California, Berkeley, School of Law. While in law school, she served as a supervising editor of the *Berkeley Journal of Criminal Law*, co-chaired the Board of Advocates, and spent three years on the trial advocacy team and two years in the Death Penalty Clinic. Both before and during law school, she worked in public defender offices in New York and California. She is now an associate at Quinn Emanuel Urquhart and Sullivan, LLP in Washington, D.C., where she works on securities litigation and white-collar criminal defense matters.