Washington Journal of Law, Technology & Arts

Volume 7 | Issue 3 Article 2

1-1-2012

Understanding and Authenticating Evidence from Social Networking Sites

Heather L. Griffith

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 7, ISSUE 3 WINTER 2012

UNDERSTANDING AND AUTHENTICATING EVIDENCE FROM SOCIAL NETWORKING SITES

Heather L. Griffith[*]

CITE AS: 7 WASH J.L. TECH. & ARTS 209 (2012)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1111

ABSTRACT

Social networking is a popular form of online interaction that combines several types of electronic communication in a single user interface. An attorney working with evidence found on social networking sites should have a general understanding of how users create and access content on social networking platforms. Before such evidence may be presented to the jury, an attorney must make a showing of authenticity. The proponent of the evidence may need to use different authentication methods depending on the type of communication involved. This Article provides background information about social networks and explores how to authenticate common types of evidence available on social networking sites.

[*] Heather L. Griffith, University of Washington School of Law, Class of 2012. Thank you to Professor Anita Krug and Articles Editor Jeff Doty for their comments and insights.

TABLE OF CONTENTS

Introduction 210
I. A Guide to Social Networking Sites 212
II. The Federal Standard for Authentication of Evidence From Social Networking Sites 214
III. Authentication of Profiles and Postings 217
A. Authentication by Distinctive Characteristics 218
B. Corroborating Non-Distinctive Characteristics on Profile Pages or Posts with Additional Evidence 220
IV. Authentication of E-mail and Chats from Social Networking Sites 221
V. Authentication of Photographs and Video from Social Networking Sites 222
Conclusion 223
Practice Pointers 223

INTRODUCTION

Social networking sites are rapidly becoming a standard method of communication for millions of users. Attorneys may find evidence of these communications useful during trial. Attorneys have sought to introduce evidence from social networking sites, including photographs to show gang affiliation,[1] posts to show witness intimidation,[2] and messages as evidence against a defendant accused of domestic violence.[3] Authentication, a prerequisite to the admission of evidence at trial, requires a showing that the evidence in question is what its proponent claims.[4]

Social networking sites present unique challenges for authentication. These sites are different than other types of electronic evidence because users create individual profile pages. Most users post identifying information on profile pages; however, social networks are pseudonymous—postings are linked to the person who

---

[1] People v. Lenihan, 911 N.Y.S.2d 588, 592 (N.Y. Sup. Ct. 2010).

[2] Griffin v. State, 19 A.3d 415, 418 (Md. 2011).

[3] People v. Goins, No. 289039, 2010 WL 199602, at *2 (Mich. Ct. App. Jan. 21, 2010).

[4] FED. R. EVID. 901(a).

posted them only through the information he or she has chosen to put on the profile. In addition, questions of who accessed and used the social networking site may arise at trial.[5] Often, the proponent must show that a particular person authored the communication, and not simply that it came from a specific social networking profile.[6]

As social networking sites become more prevalent, litigators must understand how to authenticate the various electronic formats presented by sites such as MySpace and Facebook. Evidence from these sites may take the form of profile pages, postings, chats, private messages, photos, or video. Authenticating evidence from these social networking sites may involve different methods, depending on the type of communication. Given the time and expense involved, the litigator must know how much foundational evidence a court will require for authentication.

Courts may authenticate evidence from social networking sites by use of distinctive characteristics, testimony of a witness with knowledge, or process testimony, such as testimony from a computer expert. Although users of these sites often fill their profile pages with individualized and distinctive content, the trend in the courts is to require more evidence than just a particularized profile page to authenticate a specific posting on the site. If the characteristics of the specific communication in question are genuinely distinctive, courts will allow circumstantial authentication based on content and context.[7] However, courts will require additional corroborating evidence if the characteristics are more general.[8]

This Article begins with a guide to understanding how users interact via social networking sites and description of the various forms of evidence on social networking sites. Next, the Article applies the standard for authenticating evidence to social networking sites. The discussion continues with methods of authentication for categories of evidence from social networking sites, including profiles and posts, e-mails and chats, and photographs and video.

---

[5] *See, e.g.*, Tienda v. State, No. PD–0312–11, 2012 WL 385381, at *3 (Tex. Crim. App. Feb. 8, 2012).

[6] *See, e.g.*, State v. Eleck, 23 A.3d 818, 824 (Conn. App. Ct. 2011).

[7] *See, e.g.*, *Tienda*, 2012 WL 385381, at *7.

[8] *See, e.g.*, Griffin v. State, 19 A.3d 415, 424 (Md. 2011).

I. A GUIDE TO SOCIAL NETWORKING SITES

Social networking sites are quickly becoming a common form of communication. MySpace and Facebook are among the most popular sites, and many other sites operate in a similar manner. This section discusses the basic setup for Facebook and MySpace and the ways users interact through these sites.[9] On traditional websites, the site's owner typically creates content and makes it available on the Web for others to view. On social networking sites, individual users create content inside a framework provided by the site's owner.

A user logs in to an account much like logging in to an e-mail account. Each user has a unique username and password that the user selects when setting up the account.[10] Most social networking sites do not verify the identity of the person creating the account.

A unique feature of social networking sites is the individual profile page.[11] This profile page is a Web page that the user maintains. Typically, profiles contain personal details, such as the user's name, birthday, gender, current city, interests, or other identifying information.[12] A picture, commonly called a "profile picture," is usually attached to the profile. Sometimes users choose to use the social network pseudonymously and do not provide accurate information or their real name on the profile.[13]

After an individual creates a profile page, she establishes connections with other people on the social network. Users connect to one another by linking their profiles to others' profile through a

---

[9] MySpace and Facebook are general-purpose social networking sites. Some sites have specific purposes: for example, LinkedIn is designed for professional networking. For a description of some of the different kinds of social networking sites not covered by this article, *see A Trial Lawyer's Guide to Social Networking Sites*, DELIBERATIONS: LAW, NEWS, AND THOUGHTS ON LITIGATION CONSULTING BY THE AMERICAN SOCIETY OF TRIAL CONSULTANTS (ASTC), http://jurylaw.typepad.com/deliberations/social_networking.html (last visited Jan. 9, 2011).

[10] *See Login Basics - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/login/basics (last visited Nov. 28, 2011).

[11] *See Griffin*, 19 A.3d at 426 n.13.

[12] *Griffin*, 19 A.3d at 420; *Editing My Profile Information - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/?page=216501321702579 (last visited Nov. 28, 2011).

[13] *Griffin*, 19 A.3d at 421.

process commonly referred to as "friending."[14] The virtual friendship is usually established by one user requesting to link to another user's page via a "friend request" and the second user confirming the friendship request.[15] Once the friendship is confirmed, a link appears on the profile page of both individuals. Some users only friend people they have met in person, while others will friend people they have met only through the online network. By establishing friendships, an individual creates a network of users with whom to interact.

There are many ways to interact with other individuals on a social networking site, including "posting" and "tagging." When "posting," users add information, links, pictures, or videos for others to see.[16] For example, John may post a link to an interesting online article, and Mary might comment on the post with her opinion of the article. Mary's comments are linked to her profile by her "profile picture" and the name on her profile page. Another type of interaction occurs when users upload content such as digital photographs, audio files, and video onto the site and then "tag" other users.[17] For example, a person might upload a photograph and then tag a sibling who also appears in the photograph. The tag creates a link from the photograph to the profile page of the sibling. Instead of being sent privately to an intended recipient, posts, and tags pages are published either publicly or to a group of "friends," depending on the user's privacy settings.[18] These interactions are recorded on the profile page, creating content on the site, and are available for others to view. A person may log in to the site to view the new content that has been created by those in her "friend" network.

Users also may interact directly with each other by sending private, e-mail-like messages or by chatting (also called instant

---

[14] *Adding Friends & Friend Requests - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/friends/requests (last visited Nov. 28, 2011).

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

[16] *How to Post and Share - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/?page=125122004234100 (last visited Nov. 28, 2011).

[17] *Tagging - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/tagging (last visited Nov. 28, 2011).

[18] *Griffin*, 19 A.3d at 420, 426 n.13; *News Feed basics - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/?page=132070650202524 (last visited Nov. 28, 2011).

messaging).[19] This third type of interaction does not create content on the profile page, but the individual receiving the e-mail or chat can connect to the profile page of the sender. Depending on a user's privacy settings, the site may retain a transcript of the chat session.

To control who may view profile page content, social networking sites have a variety of privacy settings.[20] Some users choose to make all or most of their content "public." This means that it is available on the Internet for anyone to see, even those who do not have an account with the social networking site. Some users make content more private by only allowing the people they have accepted as "friends" to see their information.[21] Users also may allow only specific friends to see certain content.

II. THE FEDERAL STANDARD FOR AUTHENTICATION OF EVIDENCE FROM SOCIAL NETWORKING SITES

An attorney seeking to introduce evidence from social networking sites must overcome the hurdle of authentication.[22] The proponent must provide foundational evidence to show that the evidence in question is what the proponent claims.[23] Authentication of evidence involves a two-step process. First, the court makes a preliminary determination of authenticity.[24] Rule 901(a) of the Federal Rules of Evidence[25] lays out the standard for the court's preliminary

---

[19] *Messages basics - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/messages/basics (last visited Nov. 28, 2011); *Basics: How to Chat - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/chat/basics (last visited Nov. 28, 2011).

[20] For a discussion on the difficulties of managing privacy on social networking sites, *see* JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 54-59 (2008).

[21] *See, e.g.*, A.B. v. State, 885 N.E.2d 1223, 1227 (Ind. 2008) (distinguishing posts made on a "private" MySpace profile from those made on a publically accessible profile); *Basic Privacy Controls - Facebook Help Center*, FACEBOOK, http://www.facebook.com/help/privacy/basic-controls (last visited Nov. 28, 2011).

[22] *See generally*, 5 JACK B. WEINSTEIN & MARGARET A. B`ERGER, WEINSTEIN'S FEDERAL EVIDENCE § 900.06 (2011). There may be other barriers to admissibility, such as the rule against hearsay. *Id.* at § 900.06[1][c][ii].

[23] FED. R. EVID. 901(a).

[24] *Id.*

[25] This section considers the standard under the Federal Rules of Evidence, but

determination, requiring "evidence [of authenticity] sufficient to support a finding that the matter in question is what its proponent claims."[26] The standard is low: the evidence of authenticity must be enough to provide a rational basis for a jury to find that it is authentic.[27] The evidence need not be conclusive and it may be circumstantial.[28] Second, after the court has made a preliminary finding that the evidence is what the proponent claims, the evidence is introduced and subject to cross examination. The jury considers the evidence and makes the ultimate determination of authenticity, weighing the evidence accordingly.[29]

Evidence from social networking sites may present challenges for authentication, but the traditional rules still apply. Rather than creating a new body of law, courts have adapted traditional methods of authentication to accommodate electronic evidence, including evidence from social networking sites.[30] Consequently, courts determine authenticity of electronic evidence "on a case-by-case basis as any other document."[31]

Rule 901(b) illustrates several ways to authenticate evidence, including "Testimony of witness with knowledge"; "Distinctive characteristics and the like"; and "Process or system."[32] An attorney may combine these approaches to authenticate a particular piece of evidence.

First, a witness may testify that the evidence is what it purports to

---

many state rules are substantially similar.

[26] FED. R. EVID. 901(a). The courts treat this as a question of conditional relevance under Rule 104(b). WEINSTEIN & BERGER, *supra* note 22, § 900.06[1][c][i].

[27] State v. Bell, No. CA2008-05-044, 2009 WL 1395857, at *3 (Ohio Ct. App. May 18, 2009), *appeal denied*, 914 N.E.2d 1064 (Ohio 2009).

[28] *Id.*; Manuel v. State, No. 12–09–00454–CR, 2011 WL 3837561, at *6 (Tex. App. Aug. 31, 2011).

[29] 4 DAVID BENDER, COMPUTER LAW: A GUIDE TO CYBERLAW AND DATA PRIVACY LAW, § 5.03[1], at 5-57 (rev. ed. 2010).

[30] *See, e.g.*, State v. Eleck, 23 A.3d 818, 823 (Conn. App. Ct. 2011); *see also* PAUL R. RICE, ELECTRONIC EVIDENCE: LAW AND PRACTICE 339 (Am. Bar Ass'n, 2d ed. 2008). The rules were meant to "[l]eave room for growth and development." FED. R. EVID. 901, advisory comm. note.

[31] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 543 (D. Md. 2007) (quoting In Re F.P., 878 A.2d 91, 95-96 (Pa. Super. Ct. 2005)).

[32] FED. R. EVID. 901(b).

be. For example, a witness may testify that he or she created the social network profile and posted the communication.[33]

Second, "[t]he characteristics of the offered item itself, considered in the light of circumstances, afford authentication techniques in great variety."[34] Courts have noted that the type of circumstantial evidence used for authentication changes with the medium of communication.[35] This method of authentication is particularly useful for evidence from social networking sites, where users often post identifying information.

Third, process or system authentication requires evidence "showing that the process or system produces an accurate result."[36] In cases involving evidence from social networking sites, a non-expert computer user provides authenticating testimony by testifying as to how she logged into the account and viewed the social network profile at issue, and that the printed copies are a true and correct representation of what she viewed.[37] Testimony by a computer expert or administrator of the social networking site may also assist in authentication,[38] such as when an expert determines that a particular computer was used to create the profile or a specific posting.[39]

In addition, if the foundation for authentication of evidence is weak, the probative value is limited. The court may exclude the evidence because "its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury."[40]

Once the court makes a preliminary determination of authenticity, the evidence is presented to the jury. The jury decides how to weigh any further concerns about the veracity of the evidence, such as those

---

[33] Griffin v. State, 19 A.3d 415, 427 (Md. 2011).

[34] FED. R. EVID. 901, advisory comm. note; *see also Lorraine*, 241 F.R.D. at 546.

[35] *Eleck*, 23 A.3d at 823.

[36] FED. R. EVID. 901(b)(9).

[37] *See, e.g.*, Dockery v. Dockery, E2009-01059-COA-R3-CV, 2009 WL 3486662, at *6 (Tenn. Ct. App. Oct. 29, 2009).

[38] *See, e.g.*, People v. Clevenstine, 891 N.Y.S.2d 511 (N.Y. App. Div. 2009), *appeal denied*, 925 N.E.2d 937 (2010); Commonwealth v. Williams, 926 N.E.2d 1162, 1172 (Mass. 2010).

[39] Griffin v. State, 19 A.3d 415, 427 (Md. 2011).

[40] FED. R. EVID. 403; WEINSTEIN & BERGER, *supra* note 22, § 900.06[2][b].

raised on cross-examination. This weighing goes to the credibility of the evidence, which is within the province of the jury, not the judge. For example, one court specified that the possibility that someone else accessed the defendant's social networking account was a question appropriately left for the jury.[41]

There are two distinct types of authentication that must occur for evidence from social networking sites. One is to authenticate the authorship of the evidence on the website, which is the focus of this Article. The other is to authenticate that the exhibit used at trial, typically a printout of the webpage, is a fair and accurate representation of what was on the computer screen. Testimony by a witness who viewed the information on the website is usually sufficient to meet the latter requirement.[42]

III. AUTHENTICATION OF PROFILES AND POSTINGS

Social networking sites differ from other types of electronic evidence because users create an individual profile page. Users often fill their profile pages with individualized and distinctive content. However, the trend in the courts is to require more evidence than just a distinctive profile page to authenticate a specific posting on the site. Often, the proponent must show that a specific person authored the writing, and not just that the writing came from that person's account. This evidence could take the form of distinctive characteristics within the specific posting itself; testimony from a witness with knowledge of the posting; process testimony, such as forensic computer evidence; or a combination of these methods.

A profile on a social networking site generally contains unique content connecting it to the person who created the page, even if the user posts under a false name. One Texas appellate court stated:

> The inherent nature of social networking websites encourages members who choose to use pseudonyms to identify themselves by posting profile pictures or descriptions of their physical appearances, personal backgrounds, and lifestyles. This type of

---

[41] *Clevenstine*, 891 N.Y.S.2d at 514.

[42] WEINSTEIN & BERGER, *supra* note 22, § 900.07[5].

> individualization is significant in authenticating a particular profile page as having been created by the person depicted in it.[43]

The court further stated that the more particular and distinctive the information is, the more likely a court will find it authentic.[44]

However, a personalized profile, by itself, is not usually enough to authenticate evidence from social networking sites.[45] The fact that a witness held and managed an account does not provide enough of a foundation for authentication; the proponent must show that the communication in question came from the witness and "not simply from her Facebook account."[46] Courts have raised concerns because social networking accounts may be compromised by hackers[47] and anyone may create a fictitious account under another's name.[48] In addition, users "frequently remain logged in to their accounts while leaving their computers and cell phones unattended,"[49] raising the likelihood of third parties creating unauthorized posts. The proponent of the evidence should address these concerns when laying the foundation for authentication.

A. Authentication by Distinctive Characteristics

A court may find a profile page authentic if the content of the page or the posting is so distinctive that it only could have been created by one particular individual. Concerns of misuse of the social networking account are alleviated because the substance of the communication is so distinctive. A Michigan case, *People v. Goins*, demonstrates how evidence from social networking sites may be

---

[43] Tienda v. State, No. 05–09–00553–CR, 2010 WL 5129722, at *5 (Tex. App. Dec. 17, 2010), *aff'd*, No. PD–0312–11, 2012 WL 385381 (Tex. Crim. App. Feb. 8, 2012).

[44] *Id.*

[45] *See, e.g.*, Griffin v. State, 19 A.3d 415 (Md. 2011); People v. Padilla, No. F056829, 2010 WL 4299091, at *19-20 (Cal. Ct. App. Nov. 1, 2010); State v. Eleck, 23 A.3d 818, 824 (Conn. App. Ct. 2011).

[46] *Eleck*, 23 A.3d at 824 (Conn. App. Ct. 2011).

[47] *Id.* at 822.

[48] *Griffin*, 19 A.3d at 421.

[49] *Eleck*, 23 A.3d at 822.

authenticated by distinctive content and context.[50] The Michigan Court of Appeals stated that "what certainly appears to be Bradley's [the victim] MySpace page" contains "descriptive details of the assault that fit within what a reasonable person would consider to be 'distinctive content' not generally known to anyone other than Bradley, defendant, or someone in whom one or the other confided."[51] The court held that these indicia were sufficient for the jury to reasonably find that Bradley was the author of the MySpace content.[52]

Similarly, in *Tienda v. State*, Texas' highest criminal court authenticated a MySpace page not only because it contained the defendant's name, nicknames, city, and numerous photographs; but because it also contained references to the crime, arrest, and subsequent electronic monitoring.[53] The court found "ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the MySpace pages belonged to the appellant and that he created and maintained them."[54] The distinctive characteristics allowed the jury to infer that it was unlikely that anyone else created the social networking profile or post.

Courts have not authenticated evidence from profile pages or posts when they contain only general information about a witness.[55] In *Griffin v. State*, Maryland's highest court held that a witness's birthday, location, photograph, and use of a nickname did not provide a foundation to authenticate the profile.[56] Information that is generally known by a witness's associates and friends is not "distinctive" and thus cannot be enough to authenticate a profile page. In this situation, the proponent may provide additional evidence

---

[50] People v. Goins, No. 289039, 2010 WL 199602, at *2 (Mich. Ct. App. Jan. 21, 2010).

[51] *Id.*

[52] *Id.*

[53] Tienda v. State, No. PD–0312–11, 2012 WL 385381, at *7 (Tex. Crim. App. Feb. 8, 2012).

[54] *Id.*

[55] *See, e.g.*, Griffin v. State, 19 A.3d 415 (Md. 2011); State v. Eleck, 23 A.3d 818, 824 (Conn. App. Ct. 2011); People v. Padilla, No. F056829, 2010 WL 4299091, at *17-18 (Cal. Ct. App. Nov. 1, 2010).

[56] *Griffin*, 19 A.3d at 424.

for authentication.

B. Corroborating Non-Distinctive Characteristics on Profile Pages or Posts with Additional Evidence

Authentication of evidence from social networking sites may require the attorney to use multiple methods of authentication. In some situations, the individualized characteristics of the profile page are not distinctive enough to allow for authentication. The proponent should introduce corroborating evidence to provide further foundation for authentication. In addition, the proponent should use process testimony to demonstrate that the printed court exhibits are true and correct representations of the Web page.

Corroborating evidence may take the form of testimony of a witness with knowledge or process testimony by a computer expert. A witness can testify that she authored a particular post, or that she saw someone author it.[57] Courts have also sought evidence relating to "who had access to the [Web] page and whether another author . . . could have virtually-penned the messages."[58] Expert computer testimony will also assist in authentication, such as by determining whether a particular computer was used to create the posting or profile in question.[59] Expert testimony can provide the court information "regarding how secure such a Web page is, who can access a My[S]pace Web page, whether codes are needed for such access, etc."[60]

Mere testimony from a person viewing a MySpace page is not sufficient to establish that the content is from a particular party.[61] The Massachusetts Supreme Court likened the electronic communication to a telephone call, saying: "a witness's testimony that he or she has received an incoming call from a person claiming to be 'A,' without more, is insufficient evidence to admit the call as a conversation with 'A.'"[62]

---

[57] *See id.* at 427.
[58] *Id.* at 425; *see also Padilla*, 2010 WL 4299091, at *19.
[59] *Id.* at 427.
[60] Commonwealth v. Williams, 926 N.E.2d 1162, 1172 (Mass. 2010).
[61] *Williams*, 926 N.E.2d at 1171; *see Griffin*, 19 A.3d at 418.
[62] *Id.*

IV. AUTHENTICATION OF E-MAIL AND CHATS FROM SOCIAL NETWORKING SITES

Other types of evidence from social networking sites are analogous to more familiar forms of electronic evidence. While jurisdictional rules may vary, courts generally have established methods for authentication of e-mail and Internet chat.[63]

Courts have compared messages sent privately between profiles on social networking sites to e-mail and traditional letters.[64] Standard e-mail messages are often authenticated either by someone with personal knowledge of the transmission (or receipt) or circumstantially through the use of distinctive characteristics.[65] Private messages sent through social networking sites may also be authenticated in the same way. For example, a California court permitted authentication based on testimony from the victim that he sent messages and received replies, and "based on their content, he believed he was communicating with the defendant."[66] When the defendant challenged the authenticity of the printouts of the messages, the court said that any possibility that the messages were written by someone else went to the weight of the evidence and left the final determination of authenticity to the jury.[67]

Chatting using social networking sites is similar to Internet chatting using other websites. Courts have permitted authentication of Internet chats by the use distinctive characteristics.[68] Chat conversations using social networking sites are linked to an individual profile page. In *State v. Bell*, an Ohio case, the information on a MySpace profile served to corroborate the distinctive characteristics contained within chat messages.[69] A witness had MySpace e-mails and online conversations with the defendant. The

---

[63] For a more detailed discussion of e-mail and chat authentication, *see generally* WEINSTEIN & BERGER, *supra* note 22, §§ 901.08[3]-[4].

[64] *See* People v. Fielding, No. C062022, 2010 WL 2473344, at *4 (Cal. Ct. App. June 18, 2010), review denied (Sept. 1, 2010).

[65] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 554-55 (D. Md. 2007).

[66] *Fielding*, 2010 WL 2473344, at *5.

[67] *Id.* at *3-5.

[68] *Lorraine*, 241 F.R.D. at 556.

[69] State v. Bell, 882 N.E.2d 502, 511 (Ohio Ct. Com. Pl. 2009), *aff'd*, No. CA 2008-05-044, 2009 WL 1395857 (Ohio Ct. App. May 18, 2009).

witness, T.W., testified that he accessed the messages by logging into his MySpace profile and that the printouts were accurate records of his conversation.[70] T.W.'s testimony was sufficient for authentication because of his knowledge of the defendant's MySpace username and the code words contained in the communications that would only be known by the defendant and T.W.[71]

In cases where communications do not contain distinctive characteristics, courts may require expert testimony or other corroborating evidence for authentication. For example, the Massachusetts Supreme Court in *Commonwealth v. Williams* held that the proponent of evidence from a MySpace account had only shown the evidence came from a particular profile page, and not from a specific person.[72] The trial court should not have admitted the evidence without additional foundational testimony.[73]

V. AUTHENTICATION OF PHOTOGRAPHS AND VIDEO FROM SOCIAL NETWORKING SITES

An individual may post digital photographs or videos on social networking sites, but they cannot be authenticated by distinctive characteristics alone. While a photograph is linked to the profile page of the person who posted it, there is nothing connecting the person who posted the photo to the place and time where the photograph was taken.[74] For example, a person may take an image from an unrelated website, copy it, and then post it on a MySpace profile. Thus, photographs from social networking sites may not be authenticated by the distinctive characteristics of a profile page.[75]

---

[70] State v. Bell, No. CA 2008-05-044, 2009 WL 1395857, at *5 (Ohio Ct. App. May 18, 2009).

[71] State v. Bell, 882 N.E.2d 502, 512 (Ohio Ct. Com. Pl. 2009), *aff'd*, No. CA 2008-05-044, 2009 WL 1395857 (Ohio Ct. App. May 18, 2009).

[72] Commonwealth v. Williams, 926 N.E.2d 1162, 1172 (Mass. 2010).

[73] *Id.*

[74] *See* People v. Ulloa, No. B223203, 2011 WL 3131022, at *6 (Cal. Ct. App. June 22, 2011); People v. Hernandez, No. B216495, 2010 WL 4983290, at *7-8 (Cal. Ct. App. Dec. 9, 2010).

[75] *See, e.g.*, People v. Beckley, 110 Cal. Rptr. 3d 362, 366 (Cal. Ct. App. 2010), *cert. denied*, 131 S.Ct. 1522 (2011); People v. Lenihan, 911 N.Y.S.2d 588, 592 (N.Y. Sup. Ct. 2010).

The two typical ways to authenticate a digital photograph, regardless of the source of the photograph, are (1) testimony from someone present at the time the photograph was taken or (2) expert testimony that the photograph was not altered.[76] Digital videos have similar standards for authentication.[77] Proponents of evidence from social networking sites should also use these standards.

CONCLUSION

Social networking websites may contain several types of electronic evidence, including profile pages, posts, private e-mail messages, chats, photographs, and video. Profiles pages, posts, messages, and chats sometimes contain distinctive characteristics that allow for authentication. This evidence must be in the specific communication at issue and distinctive enough to show who authored the communication. If the evidence does not contain distinctive characteristics, the court will require additional foundational evidence for authentication, such as testimony of a witness with knowledge or testimony from a computer expert. Proper foundational evidence will help the proponent of the evidence properly authenticate evidence from social networking sites.

PRACTICE POINTERS

- Attorneys need to understand the type of electronic evidence they are authenticating. Evidence from social networking sites may include profile pages, chat transcripts, public messages, private e-mail-type messages, digital photographs, or video.
- Users of social networks often post identifying information. If this information contains unique and distinctive characteristics, it may be used to aid authentication.
- If the information posted on the social networking site is generally known in the user's community, it is not sufficient for authentication and additional foundational evidence is

---

[76] *Beckley*, 110 Cal. Rptr. 3d at 366-67, *see also* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 561-62 (D. Md. 2007).

[77] *See* WEINSTEIN & BERGER, *supra* note 22, § 901.05[1].

required. This may take the form of testimony of a person with knowledge of who posted the information, a computer expert, or a person from the company that runs the social networking site.

- The person who accessed the social networking site should testify as to how the page was accessed. This witness should also verify that the printouts used in court are a true and accurate copy of what the witness saw on the computer screen.
- Photographs and video taken from social networking sites cannot be authenticated by distinctive characteristics of a profile page. The standard methods for authentication of photographs and video still apply.
- The possibility that another party accessed and used an account usually goes to the weight of the evidence, not admissibility.