From the SelectedWorks of M. Anderson Berry

January 1, 2010

Voodoo Information: Authenticating Web Pages in Federal Court

M. Anderson Berry
David Kiernan

Available at: https://works.bepress.com/m_berry/7/
By M. Anderson Berry and David Kiernan

Plaintiff sues your client, claiming that his injuries have significantly affected his lifestyle. He is unable to work, travel or bowl. Not surprisingly, his spouse alleges loss of consortium. On the eve of trial, you discover pictures and other details on a social networking Web site about plaintiff’s recent trip to the International Bowling Museum & Hall of Fame, including a picture of plaintiff proudly holding a fluorescent orange bowling ball and a four-foot tall gilded trophy dated four days earlier. As you approach the witness with printouts of the Web pages, you are stopped in your tracks: “Objection, lack of foundation.”

It is now routine for litigators to conduct Internet research to work up a case. Indeed, for many litigators, one of the first things they do is see what is available about the opposing party, searching Google, social networking sites like Twitter, MySpace and Facebook, and the party’s personal Web sites. During the life of any case, there will likely be valuable information obtained from the Internet that will be used at deposition or trial. Commonly, the proponent of online evidence will present a screen shot of the Web page, which was either downloaded as a .pdf or printed directly from the Web site. The process is like taking a photograph of the image as it appears on the monitor. In general, this captures not only the look, but also the download date and the URL. If proper steps are not taken to admit the evidence, the value of this information may be lost.

**Issues of Length, Originality**

Starting with the issue of length, the Office of Copyright’s Circular 34 states that “names, titles, and short phrases or expressions are...”

‘Voodoo Information’: Authenticating Web Pages In Federal Court

By M. Anderson Berry and David Kiernan

Plaintiff sues your client, claiming that his injuries have significantly affected his lifestyle. He is unable to work, travel or bowl. Not surprisingly, his spouse alleges loss of consortium. On the eve of trial, you discover pictures and other details on a social networking Web site about plaintiff’s recent trip to the International Bowling Museum & Hall of Fame, including a picture of plaintiff proudly holding a fluorescent orange bowling ball and a four-foot tall gilded trophy dated four days earlier. As you approach the witness with printouts of the Web pages, you are stopped in your tracks: “Objection, lack of foundation.”

It is now routine for litigators to conduct Internet research to work up a case. Indeed, for many litigators, one of the first things they do is see what is available about the opposing party, searching Google, social networking sites like Twitter, MySpace and Facebook, and the party’s personal Web sites. During the life of any case, there will likely be valuable information obtained from the Internet that will be used at deposition or trial. Commonly, the proponent of online evidence will present a screen shot of the Web page, which was either downloaded as a .pdf or printed directly from the Web site. The process is like taking a photograph of the image as it appears on the monitor. In general, this captures not only the look, but also the download date and the URL. If proper steps are not taken to admit the evidence, the value of this information may be lost.

**AUTHENTICITY**

As with all evidence, the proponent must be prepared to establish that the evidence is relevant, authentic, and not subject to exclusion under the hearsay or best evidence rules. This article focuses on the second evidentiary hurdle: authenticity. Although the burden of authenticating a document is usually quite low, doing so for a screen shot of a Web site presents an additional challenge, as courts generally view such information with suspicion. As one federal district judge noted: “Anyone can put anything on the Internet. ... [The Internet is] one large catalyst for rumor, innuendo, and misinformation.” St. Clair v. Johnny’s Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774-75 (S.D. Tex. 1999). It is “voodoo information.” Id.

**In This Issue**

Authenticating Web Pages in Federal Court ........1
Copyright in Tweets ...1
Evidence on Social Networking Sites .......3

continued on page 5
‘Voodoo Information’
continued from page 1

AUTHENTICATION UNDER FEDERAL RULE OF EVIDENCE 901

Federal Rule of Evidence (“FRE”) 901(a) requires the proponent to show that the evidence is what it is purported to be. Notably, the proponent need only make a prima facie showing from which the jury could reasonably find that the document is authentic. Most courts require the proponent to come forward with “admissible evidence” to lay the foundation, reasoning that the court's authenticity determination is governed by FRE 104(b). See, Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 539-40 (D. Md. 2007).

FRE 901(b) provides a non-exhaustive list of illustrations of how a proponent may authenticate a document. The two candidates for authenticating screen shots are 901(b)(1) (permitting authentication by “[t]estimony that a matter is what it is claimed to be”) and 901(b)(4) (permitting authentication by “[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances”). Reflecting their suspicion of “voodoo information,” the majority of courts appear to require the proponent to authenticate a Web site under 901(b)(1). As one commentator has noted, testimony must answer the following questions: “1) What was actually on the Web site? 2) Does the exhibit or testimony accurately reflect it? and 3) If so, is it attributable to the owner of the site?” Lorraine, 241 F.R.D. at 555-56 (quoting Gregory P. Joseph, Internet and Email Evidence, reprinted in 5 Stephen A. Saltzburg et al., Fed. R. Evid.

David C. Kiernan (dkiernan@jonesday.com) is a litigator in the Trial Practice Group of Jones Day in its San Francisco Office and is a member of the firm’s E-Discovery Committee. M. Anderson Berry (aberry@jonesday.com) is also an attorney in the same office. The views expressed are solely those of the authors and should not be attributed to the authors’ firm or its clients.

Man., Part 4 at 20 (9th ed. 2006). That same commentator provides a list of factors that a court may consider, including the “length of time the data was posted on the site … whether it remains on the Web site for the court to verify; whether the data is of a type ordinarily posted on that Web site or Web sites of similar entities … whether the owner of the site has elsewhere published the same data, in whole or in part; … whether the data has been re-published by others who identify the source of the data as the Web site in question.” Id.

Courts generally fall into three camps with respect to the scope of testimony that 901(b)(1) requires. The first camp requires testimony showing that the information was posted by the individual to whom the information is attributed in the form of a “statement or affidavit from … [the Web site’s] [W]eb master or someone else with personal knowledge.” In re Homestore, Inc. Sec. Litig., 347 F. Supp. 2d 769, 782-83 (C.D. Cal. 2004); see also, Waddy v. Provident Life and Accident Ins. Co. of Am., 216 F. Supp. 2d 1060 (C.D. Cal. 2002) (sustaining objection to affidavit because affiant lacked personal knowledge of who maintained the Web site or authored the documents). This is akin to authenticating a letter, which requires showing that it was written by the individual to whom it is attributed.

The second camp is much more permissive, finding sufficient testimony from the person who created the screen shot that the image “accurately reflects the contents of the Web site and the image of the page on the computer at which the [screen shot] was made.” Toytrackers, LLC v. Koehler, 2009 WL 2591329, at 6 (D.Kan. Aug. 21, 2009); see also, Nightlight Sys., Inc. v. Nitelles Franchise Sys., Inc., 2007 WL 4563875, at 5-6 (N.D. Ga. May 11, 2007). The standard applied by these courts is not much different from that applied to photographs. In kSolo, Inc. v. Catona, for example, the court admitted a screen shot, noting that although the declarant “may not have [had] knowledge as to how the Web site works on a technological level, his declaration establishes sufficient knowledge

continued on page 6

INTERNET LAW & STRATEGY®
Evidence on Social Networking Sites

By Ken Strutin

Social networking sites offer an abundance of exculpatory and impeaching evidence that may not be obtainable without some undercover detective work. Unfortunately, discovery rules and ethical guidelines have not kept pace with the digital sprawl of MySpace and Facebook. In the absence of explicit direction from the Rules of Professional Conduct and the laws governing online behavior, flying a false flag in these uncharted waters may be hazardous. See generally, “Pretexting, Legal Ethics and Social Networking Sites,” LLRX, Oct. 5, 2009.

Deceptive Practices

Before an attorney or investigator considers using subterfuge — such as concealing his or her true identity and purpose to contact a witness through an online profile — he or she ought to be mindful that legal and ethical precedents on this subject are slow in coming.

Historically, surreptitious investigation has found some validation in the arenas of law enforcement, civil rights and intellectual property infringement. Still, there is a scarcity of ethical and legal authorities outside these specific areas and only recently has online covert investigation begun to draw attention.

In March, the Philadelphia Bar Association’s Professional Guidance Committee issued what appears to be the first ethics opinion (2009-02) categorically proscribing lawyers and their associates from using deception in connection with contacting a deponent through her online profiles.

A witness in a civil case revealed during her deposition that she had Facebook and MySpace accounts. The attorney seeking the ethics opinion believed these sites contained information relevant to the case and, in particular, valuable for impeachment. No direct questions were posed to the witness about the contents of the accounts.

Access to the witness’ pages was by permission only. The attorney asked the committee whether it would be allowable to ask someone to “friend” the witness without disclosing his affiliation or purpose. All identifying and other information would be truthful.

Noting the responsibility of lawyers for the behavior of investigators, the committee found that the proposed actions would constitute misconduct under Rule 8.4 prohibiting “dishonesty, fraud, deceit or misrepresentation.” Therefore, “friending” the witness without revealing that the purpose of the contact was to gain access to private areas of her profile constituted an act of “deception.”

The lawyer’s concern over the witness’ reluctance to otherwise permit access did not soften the nature of the concealment. Even if the witness had a liberal practice of accepting friend requests, running the risk that someone might take advantage of the information in her profiles, it did not temper the result.

Acknowledging the conflicting views on covert investigation, the committee declined to recognize an exception along the lines of the ones found in New York and other states ethics opinions and court decisions.

New York Exception

In Opinion 737, the New York County Lawyers’ Association’s Committee on Professional Ethics developed this approach in response to a question about private attorney pretexting:

Non-government attorneys may … ethically supervise non-attorney investigators employing a limited amount of dissemblance in some strictly limited circumstances where: 1) either a) the investigation is of a violation of civil rights or intellectual property rights and the lawyer believes in good faith that such violation is taking place or will take place imminently, or b) the dissemblance is expressly authorized by law; 2) the evidence sought is not reasonably available through other lawful means; 3) the lawyer's conduct and the investigators’ conduct that the lawyer is supervising do not otherwise violate the Code (including, but not limited to, DR 7-104, the “no-contact” rule) or applicable law; and 4) the dissemblance does not unlawfully or unethically violate the rights of third parties.

Notably, “dissemblance” in this context included concealment or misstatement of identity and purpose in the process of evidence gathering.

The New Privacy

The online social media phenomenon begs the question: How private is a social networking profile where a friend’s list could fill Yankee Stadium? See, “How Many Friends Is Too Many?” Newsweek, May 26, 2008. Online culture is an estate of compromise, where privacy gives ground to community building. A social network cannot function unless its members relinquish some personal space-making obscurity as a substitute for privacy. In essence, social networking sites are quasi-public.

Studies have illustrated that users seeking to create online identities, form relationships or join networks knowingly expose themselves and their friends and families to the scrutiny of people they have never met or intended to meet. See generally, “Saving Facebook,” 94 Iowa L. Rev 1137, 1197 (2009). And it carries implications for the practice of law. For example, a Canadian judge observed that a litigant with 366 friends could not contend that his profile was intended to be private. See, Murphy v. Perger, (2007) O.J. No. 5511 (Ontario Super. Ct Just. Oct. 3, 2007); see generally, “Fessing Up to Facebook: Recent Trends in the Use of Social Network [Web sites] for Insurance Litigation,” SSRN, March 3, 2009, at 6 (available at http://ssrn.com/abstract=1352670).

The reality of public privacy in social networking sites blunts the absolutist view of online privacy underlying the Philadelphia bar committee’s opinion.

Criminal Law Practice

The lodestars of due process, effective assistance of counsel and the right to present a defense, guide every criminal defense investigation and discovery request. Yet, the ethical and legal exceptions carved out for undercover work have not directly addressed these constitutional beacons. Are a defendant’s rights to counsel and due process less important than continued on page 4

Ken Strutin is director of legal information services at the New York State Defenders Association (www.nysda.org).
uncovering housing discrimination or trademark infringement?

In the absence of clear-cut guidelines or precedent, covert online investigation must be analyzed on a case-by-case basis. In an oft-cited law review article, attorneys David B. Isbell and Lucantonio N. Salvi developed a framework for examining these issues that might be useful in future cases. See, “Ethical Responsibility of Lawyers for Deception by Undercover Investigators and Discrimination Testers,” 8 Geo. J. Legal Ethics 791 (1995).

Their analysis begins with the premise that undercover investigations performed by private attorneys and their employees or associates are aimed toward a laudable purpose or societal good.

In the criminal context, this translates into the prevention of wrongful conviction and promotion of fair trials. Effectively representing an accused and presenting a defense are essential to the administration of justice and the stability of society. See generally, “Final Report of the New York State Bar Association’s Task Force on Wrongful Convictions” (April 4, 2009); and “Strengthening Forensic Science in the United States: A Path Forward” (N.R.C. 2009).

Next, the evidence to be gathered could not be acquired by other means, e.g., discrimination testing.

The content on social networking sites is as unique as the people who post it. And like all online sources, these profiles are transitory and their content easily altered or removed. In other words, they may contain evidence “not reasonably available through other lawful means.” Isbell and Salvi’s thorough and insightful interpretation of the model rules led them to conclude:

The pertinent rules simply do not prohibit a lawyer’s involvement with testers or investigators making misrepresentations only of the kinds here under consideration — namely, misrepresentations as to identity or purpose, made solely for purposes of discovering information. “Ethical Responsibility,” 8 Geo. J. Legal Ethics at 811.

Of course, this analysis did not conclude a blanket exemption. The “nature of the misrepresentations” and the “circumstances in which they are made” are always factors. According to the authors, if the dissembling was limited to identity and purpose in order to collect information to be used in litigation, no violence was done to the model rules. Id. at 829.

At this point, no authority has squarely addressed this question in the context of defense investigation of online social networking profiles.

RECIPROCAL DISCOVERY

Still, there are many compelling reasons for undercover discovery of digital and online evidence, such as exploring the veracity of a government witness. See, e.g., NYSBA Comm. on Prof. Ethics Op. 402 (1975) (not improper to employ investigator to befriend key prosecution witness to ascertain truthfulness of testimony).

In Office of Lawyer Regulation v. Hurley, No. 2007AP478-D (Wis. Sup. Ct. Feb. 11, 2009), a Wisconsin attorney confronted the ethical quandaries raised by using undercover investigation in a case where the victim claimed the defendant forced him to view child pornography. The attorney sought exculpatory material from the complainant’s computer to show that he had the ability and inclination to view illicit images on his own.

The lawyer suspected that if put on notice, the complainant might destroy information on his computer that would expose his misconduct. He hired a private investigator to carry out a pretense, a computer swap offer, to acquire the victim’s laptop temporarily for examination. Forensic analysis revealed many illicit pornographic images.

A complaint was filed against the attorney for violating the equivalent of Rule 4.1, making a false statement to a third person, and Rule 8.3, engaging in dishonesty, fraud, deceit or misrepresentation.

Ultimately, the Supreme Court of Wisconsin affirmed a referee’s finding that the attorney had not violated any ethics rules. There was no rational distinction between the prosecutor’s use of undercover investigative techniques and the defense need to acquire information in pursuit of their client’s constitutional rights. Recognizing the deference accorded law enforcement in utilizing deception in criminal investigations, the court found:

Neither of them [Director of Office of Lawyer Regulation or Prosecutor] could point to any Wisconsin precedent drawing a distinction between prosecutors and other attorneys in that regard, and the record demonstrates that there was wide belief in the Wisconsin Bar that the type of conduct engaged in by Attorney Hurley was acceptable.

In an article reviewing developments in this area of ethics, the author questioned the efficacy of the Philadelphia bar committee opinion against the background of New York and Wisconsin’s treatment of similar issues:

The Hurley case may supply an argument justifying the conduct of one pretexting attorney, expanding on NYC Bar Op. 2003-2 [undisclosed taping of conversations by lawyers] and NYCLA Op. 737 [non-government lawyer use of investigator who employs dissemblance], but it may not be an airtight defense to discipline that will apply in all situations. See, “Report on Pretexting — Recent Cases & Ethics Opinions,” NY Prof. Resp. Rept., June 2009, at 1, 10.

REPERCUSSIONS

Disciplinary sanctions, criminal charges for violating terms of use or other federal laws (compare “First ‘Pretexting’ Charges Filed Under Law Passed After HP Spy Scandal,” Wired, Jan. 9, 2009 with “Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury,” Wired, July 2, 2009), not to mention the possible suppression of evidence at trial, are a few of the risks inherent in this kind of investigation. See, e.g., Stagg v. New York City Health & Hosp. Corp., 162 A.D.2d 595 (2nd Dep’t 1990); and United States v. Hammad, 858 F.2d 854 (2d Cir. 1988) (“government should not have its case prejudiced by suppression of its evidence when the law was previously unsettled in this area”).

On the other hand, case preparation that overlooks social networking evidence may expose an attorney
Copyright in Tweets
continued from page 1

not subject to copyright protection," even if they are "novel or distinctive." At 140 characters, a tweet is likely to be seen as a short phrase or expression. There is ample case law demonstrating that size matters in copyright protection and deferring to the government circular. (See, e.g., N.Y. Mercantile Exch., Inc. v. IntercontinentalExchange, Inc., 389 F. Supp. 2d 527 (S.D.N.Y. 2005).)

Still, certain written expressions, like haikus, are certainly worthy of copyright protection in spite of their diminutive length. (See, Applied Innovations, Inc. v. Regents of the University of Minnesota and National Computer Systems, Inc., 876 F.2d 626, (8th Cir. 1989).) Could not a tweet be sufficiently original that despite its short length, it would receive copyright protection? The bulk of tweets are unoriginal or even factual in nature. They comment on the weather, what a person is doing on an hourly basis, or observations about world events. Copyright would not protect a tweet that reports "just voted no for 'Does Obama deserve the Nobel Peace Prize'" or "Obama pondering whether to send more troops to Afghanistan. I am pondering too." See, Feist Publications, Inc. v. Rural Telephone Service Co., 499 U.S. 340 (1991) (holding that facts are not protected by copyright, only that aspect of the work that displays the author's originality).

Since copyright law essentially grants a monopoly over an arrangement of words, courts will be loathe to protect a simple expression of fact that varies only slightly from another simple expression of fact. In Landsberg v. Scrabble Crossword Players, Inc., et. al., 736 F. 2d 485 (1984), the Ninth Circuit Court of Appeals decided that a manual for Scrabble® was not copyright pro-
tected because it largely contained factual information about the game. The court explained: "Factual works are different [from fictional works]. Subsequent authors wishing to express the ideas contained in a factual work often can choose from only a narrow range of expression." Tweets by their factual nature are unlikely to be protected by copyright.

In addition, the shorter the expression, the harder it is to establish originality and creativity. 2 Melville B. Nimmer & David Nimmer, Nimmer on Copyright §2.01[B] (MB, Rev. Ed., discussing 37 C.F.R. Section 202.1(a) that denies copyright protection to short phrases like slogans, "it would seem (notwithstanding the above quoted Copyright Office Regulation) that even a short phrase may command copyright protection if it exhibits sufficient creativity. ... There is a reciprocal relationship between creativity and independent effort. The smaller the effort (e.g., two words) the greater must be the degree of creativity in order to claim copyright protection." See also, Identity Arts v. Best Buy Enter. Serv., Inc., 2007 U.S. Dist. LEXIS 32060; Narell v. Freeman, 872 F.2d 907, 911 (9th Cir. 1989) ("ordinary phrases are not entitled to copyright protection").

TWEET PROTECTION

If, however, there were a hypothetical tweet that was sufficiently creative and original to warrant copyright protection, the next question is how would the tweeter protect it? While the copyright could exist from the moment the writing is fixed on the server, it takes a registration to enforce such a copyright and prevent third-party use. It is not feasible to register each tweet that a person composes, nor do we know the Copyright Office's position on granting registrations of tweets. It is more practical that one could register a compilation of tweets. Some tweeters, therefore, have been blogging about filing registrations every few months that cover all their tweets in the time period. Since, however, it is unlikely that a single tweet is worthy of copyright protection, it will be even more difficult to have written three months’ worth of original, creative tweets. It is likely that the compilation's copyright, then, would cover the format of the overall compilation rather than the tweets contained in the compilation. See, Feist Publications v. Rural Telephone Service Co., Inc., 499 U.S. 340 (1991); and Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539 (1985).

Does that mean that one could create a work that compiled all tweets on the subject of President Obama winning the Nobel Peace Prize without giving attribution to the authors of factual tweets? If most tweets are too factual, too unoriginal, or too short to be protected by copyright, can anyone copy a tweet? In answering these questions, there may be issues of privacy, libel, trademark or unfair competition (which we will not explore in this article), but it is unlikely that copyright law will serve to prevent the copying.

A FAIR USE DEFENSE?

What of that rare tweet that could be protected by copyright law? Would a third-party user be able to mount a fair use defense? The factors in determining whether a fair use has been made are outlined in 17 U.S.C. §107.

The first factor is the "purpose and character of the use." Using a tweet in a news story is likely a fair use. Mark Cuban's tweet fell into the category of news, and use of the tweet would be protected just the way news disseminators may use a private letter to which they obtain access.

The second factor for determining whether there has been a fair use is the nature of the work. Given the social nature of Twitter and its users, there is a strong public policy argument that the users of Twitter mean to publicize their utterances. Another factor, the effect of the use on the underlying work's potential market or value, also cuts in favor of a fair use defense. There is limited, if any, market value to a single tweet. The tweeter would bear the burden to prove his tweet has any commercial value. Of course, this could be different if an entire compilation of tweets were taken without attribution. Then the remaining factor in the fair use analysis — "the amount and substantiality of the portion used in relation to continued on page 8
'Voodoo Information'
continued from page 2

to attest that the screen shots are an accurate representation of what he encountered upon visiting the Web site.” 2008 WL 4906115, at 1, n.5 (C.D. Cal. Nov. 10, 2008); see also, Victaulic Co. v. Tieman, 499 F.3d 227, 236 (3d Cir. 2007) (ignoring the “Web master” portion of Homestore and citing that case only for the proposition: “To be authenticated, some statement or affidavit from someone with knowledge is required”).

Notably, courts in the second camp do not appear to require the proponent to authenticate the information as authored or sponsored by the individual to whom it is attributed. Instead, the party need only show that the screen shot reflects what was on the site. Presumably, the issue of authorship or sponsorship will be the subject of cross-examination and further proof.

The third camp is somewhere in between, requiring different evidence depending on the circumstances. In United States v. Jackson, for example, the Seventh Circuit excluded screen shots because the proponent did not prove that the Web site’s owner actually posted the information. 208 F.3d 633, 637 (7th Cir. 2000). The court held that the proponent must demonstrate that the information was actually put on the Web site by the site’s sponsor. But the Jackson court went on to note that the type of evidence required to meet the prima facie burden depends on the proponent’s incentive and ability to falsify evidence. In that case, the proponent argued that a white supremacist group had claimed responsibility on its Web site for her alleged actions. Siding with the government, the court refused to admit screen shots of the supremacist group’s Web site introduced by defendant, noting that the defendant was a sophisticated computer user and had every incentive to try to place the blame on someone else. This incentive required the defendant to link the information directly to the Web site’s sponsor.

A litigant could try to authenticate a screen shot without testimony by relying on FRE 901(b)(4), arguing that the look of the screen shot, the download dates and identifying Web addresses are sufficient circumstantial evidence of authenticity. See, e.g., Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F.Supp.2d 1146, 1154 (C.D.Cal. 2002) (admitting Web site posting due to circumstantial indicia of authenticity, including presence of download dates and identifying Web addresses). However, that information is not likely to pass muster. Even in Perfect 10,

Most courts that have addressed the issue have admitted screen shots from the Wayback Machine …

the proponent submitted a declaration stating that the screen shots were true and correct copies that he printed from the Internet.

AUTHENTICATION OF SCREEN SHOTS FROM ARCHIVE.ORG

Many litigators are familiar with the Internet Archive (www.archive.org), also known as the “Wayback Machine.” The Internet Archive uses a process called crawling to visit Web sites and systematically duplicate and store the data on its own servers, which allows users to retrieve copies of Web pages as they existed at various times in the past. With the amount of information posted on the Web, it is an indispensable investigatory tool.

Most courts that have addressed the issue have admitted screen shots from the Wayback Machine, finding sufficient “a statement or affidavit from an Internet Archive representative with personal knowledge of the contents of the Internet Archive Web site.” St. Luke’s Cataract and Laser Institute, P.A. v. Sandersen, 2006 WL 1320242, at 2 (M.D Fla. May 12, 2006); Telewizja Polska USA, Inc. v. EchoStar Satellite Corp., 2004 WL 2367740, at 5-6 (N.D.Ill. Oct. 15, 2004) (party submitted affidavit from the administrative director for the Internet Archive describing in detail the process used to allow visitors to search archived Web pages). Notably, California has recognized it as an official library for purposes of federal funding.

At least one court has suggested, however, that it would not accept screen shots from the Internet Archive even if authenticated by such an affidavit. Novak v. Tucows, Inc., 2007 WL 922306, at 5 (E.D.N.Y. March 26, 2007). The court reasoned that the Internet Archive’s employees play no role in ensuring that archived Web sites accurately represent what had been posted on the original Web site. However, a recent district court case in the Second Circuit has called Novak’s dicta into question, noting that screen shots from the Internet Archive may be “authenticated by a knowledgeable employee of the Web site.” Audi AG v. Shokan Coachworks, Inc., 592 F. Supp. 2d 246, 277-78 (N.D.N.Y. 2008).


SECONDS AUTHENTICATION UNDER FRE 902

A proponent may also try to fit the screen shots into the relatively narrow categories of FRE 902, which permits authentication without extrinsic evidence. The likely candidates are 902(5) (Official Publications), 902(6) (Newspapers and Periodicals), 902(11) (Certified Domestic Records of Regularly Conducted Activity), and 902(12) (Certified Foreign Records of Regularly Conducted Activity). With respect to 902(11) and (12), the proponent will have to obtain a declaration from a qualified person certifying that the information posted on the Web site meet the requirements of a business record.

FRE 902(5) defines “Official Publications” as “[b]ooks, pamphlets, or other publications purporting to be issued by public authority.” Most courts have held, depending on the information, that screen shots of U.S. and State government Web sites are self-authenticating as an official government publication under 902(5). Paralyzed Veterans of Am. v. McPherson, 2008 WL 4183981, at 7 (N.D. Cal. 2008) (citing cases); Lorraine v. Markel Am. Ins. Co., 241 F.R.D. at 551 (“Given the frequency with which official publications from government agencies are continued on page 7
realtornant to litigation and the increasing tendency for such agencies to have their own Web sites, FRE 902(5) provides a very useful method for authenticating these publications.

No case has addressed whether screen shots from a foreign government’s Web site are self-authenticating under 902(5). Given the text of the rule, a court is likely to find that such documents are covered. FRE 902(5) provides that “publications purporting to be issued by public authority” are self-authenticating. The term “public authority” is not defined in the rules. However, courts interpreting FRE 803(8) — the hearsay exception for “[p]ublic records and reports” — have ruled that it covers “statements” by a foreign government. See, e.g., F.A.A. v. Landy, 705 F.2d 624, 633 (2d Cir. 1983) (admitting a telex sent by the German government through the U.S. State Department to the Federal Aviation Administration). Presumably, courts would read “public” to have the same scope under 902(5).

Under certain circumstances, a party may also be able to rely upon 902(3), which provides that foreign public documents are self-authenticating, even without certification. See, e.g., U.S. v. Torres-Reyes, 2002 WL 31019363, at 1 (10th Cir. 2002) (affirming the authentication of a foreign public document without certification — this case did not involve information from a Web site).

**Judicial Notice of Web Sites or Facts Contained Therein**

It may be possible to avoid the burden of authentication by requesting the court to take judicial notice of information found on a Web site. Indeed, “[i]t is not uncommon for courts to take judicial notice of factual information found on the world wide Web.” O’Toole v. Northrop Grumman Corp., 499 F.3d 1218, 1225 (10th Cir. 2007); see also, Hotel Employees & Restaurant Employees Union, Local 100 of New York, N.Y. & Vicinity, AFL CIO v. City of New York Dept. of Parks & Recreation, 311 F.3d 534, 549 (2d Cir. 2002).

Federal Rule of Evidence 201(b) provides: “A judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned.” Id. If the information is relevant, it is “appropriate to take [judicial] notice of the fact that the Web site makes such a designation, [if] the authenticity of the site has not been questioned.” Hotel Employees, 311 F.3d at 549; see also, Francarly Realty Corp. v. Town of East Hampton, 628 F. Supp. 2d 329, 332 (E.D.N.Y. 2009). Moreover, FRE 201(d) makes the rule mandatory when it applies.

In O’Toole, the district court denied plaintiff’s request to take judicial notice of relevant facts listed on Northrop’s Web site. Plaintiff had supplied the court with the address for the Web page, and the court located it online. Id. The Tenth Circuit found that the district court had abused its discretion by not judicially noticing the facts found on Northrop’s Web site, finding that O’Toole “addressed all the factors relevant to the application of [FRE] 201(b)(2).” Id. The court noted that Northrop had not raised any reasonable dispute that the information was unreliable. Id. at 1225; see also, Wang v. Pataki, 396 F. Supp. 2d 446, 458 (S.D.N.Y. 2005) (taking judicial notice of information on a non-party’s Web site).

Similarly, in Paralyzed Veterans of America, plaintiffs supplied to the court the applicable Web pages that appeared on the California Secretary of State’s Web site. The first Web page included a letter approving a California county’s use of the vote-counting device at issue in the litigation. The second page listed a set of conditions on the use of the device. The court took judicial notice of the information on both Web pages on the grounds that defendants did not reasonably question the Web site’s accuracy and the information was capable of accurate and ready determination online.

At least one circuit court has required more before taking judicial notice of information on a Web site. In Vicaulic Co. v. Tieman, the district court had established certain facts about plaintiffs by accessing defendants’ Web site, which was not disputed as inauthentic by defendants. 499 F.3d 227, 236 (3d Cir. 2007). The Third Circuit, however, held that the opposing party is not required to dispute the authenticity of the Web site, noting that “we allow judicial notice only from sources not reasonably subject to dispute.” Id. (citing FRE 201(b)) (emphasis added). The court found that judicial notice was improper here because “[a]nonyone may purchase an [I]nternet address, and so, without proceeding to discovery or some other means of authentication, it is premature to assume that a [W]ebsite page is owned by a company merely because its trade name appears in the [URL].” Id. Given the suspicion many courts hold toward information posted on the Internet, a party in the Third Circuit faces an uphill battle.

**Conclusion**

Although many courts view Internet evidence as “voodoo information,” with the proper support, authentication should be overcome; overcoming a hearsay objection may be the real challenge. To authenticate a screen shot, the proponent of a screen shot should try to obtain testimony through affidavit, requests for admission, deposition or live testimony from the Web site’s sponsor or Web master. At a minimum, the proponent must obtain from the individual who took the screen shot testimony stating that the image accurately reflects the content of the Web site and the image of the page on the computer at which the screen shot was made. The best practice would be to draft a declaration immediately after the individual obtains the screen shot. If the evidence is from the opposing party’s Web site, the litigant should try to authenticate at the party’s deposition or through a request for admission. And the parties are always free to stipulate to authentication of any documents, including screen shots. Finally, requesting judicial notice should be considered, depending, of course, on the jurisdiction.

❖

The publisher of this newsletter is not engaged in rendering legal, accounting, financial, investment advisory or other professional services, and this publication is not meant to constitute legal, accounting, financial, investment advisory or other professional assistance. If legal, financial, investment advisory or other professional assistance is required, the services of a competent professional person should be sought.
Copyright in Tweets

the copyrighted work as a whole — could trump an invocation of the defense.

Commercial Gain

The more difficult case comes in using a tweet for commercial gain. For example, what would happen if an entire compilation of tweets by a celebrity were published without permission or attribution? If a celebrity were to mention a product in her tweet, and then the company selling the product used the tweet without permission in its advertising, would copyright help the celebrity? Again, it is more likely that privacy law and advertising law principles governing testimonials would be at issue. Only if one can prove an underlying valid copyright in the tweet would we come to an analysis of the case law on commercial speech. See, Cent. Hudson Gas & Elec. Corp. v. Public Serv. Comm’n, 447 U.S. 557 and its progeny. Then, a case-by-case analysis would be necessary to see whether a fair use defense could be mounted. See, Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 577 (1994) (on applying a case-by-case analysis to a fair use defense).

Social Networking

to malpractice or ineffectiveness of counsel claims. See, e.g., People v Bennett, 29 N.Y.2d 462, 467 (1972); accord Lindstadt v. Keane, 239 F.3d 191, 201 (2nd Cir. 2001).

The unevenness of authorities on this point puts defense counsel on the horns of a constitutional dilemma.


In Wardius v. Oregon, 412 U.S. 470 (1973), the conviction was overturned due to an unbalanced alibi evidence rule that did “not” allow the defense reciprocal discovery of the state’s rebuttal witnesses.

And based on the right to present a defense, the Court in Chambers v. Mississippi, 410 U.S. 284, 302 (1973), held that a hearsay rule prohibiting introduction of exculpatory evidence of third party guilt violated due process.

Last, a rule barring a co-participant’s testimony in Washington v. Texas, 388 U.S. 14, 19 (1967), while allowing the prosecution the exclusive privilege to present such evidence, ran afoul of the compulsory process clause.

These cases reveal the overarching principles of fairness and reciprocal discovery that ought to apply with equal force to the cyber-extended society created by and accessible to hundreds of millions of people.

Links to Tweets, Tweetbacks

What about links to tweets and tweetbacks? (Tweetbacks are automated systems that collect and republish tweets all on one topic.) Are these systems guilty of scraping? Scraping refers to automated software that searches for content and then copies it on another site. For example, a site that compares prices of a product on the Internet may scrape other sites for information and republish for price comparisons. If the material being scraped is protected by copyright, then the scraping could be unlawful. Given that most tweets are not protected by copyright, the scraping offense would not apply.

To the rare tweet that is protected by copyright, the fact that third parties are availing themselves of Twitter’s Application Programming Interface (“API”) and complying with its terms of service would likely eliminate scraping as a copyright violation. See, Field v. Google Inc., 412 F. Supp. 2d 1106 (2006) (holding that automated, non-volitional conduct by a search engine’s computers in response to users’ requests to access copies of copyrighted works that were cached by the search engine did not constitute copyright infringement; invoking safe harbor provision relating to online material of Copyright Act).

Twitter has a draft set of rules for developers of software that interact with Twitter’s API. These draft rules suggest that such companies must provide attribution of authorship for any tweets they use, “maintain the integrity of Tweets” by not editing or altering them, obtain the tweeter’s “consent before sending Tweets or other messages on their behalf,” and finally, “get permission from the [tweeter] if you want to make their Tweet into a commercial good or product.” While this set of rules has not been formalized, it functions as a set of guidelines for those interacting with the API to preclude a copyright claim as well as a host of other legal claims.

Conclusion

Determining whether copyright law protects a particular tweet is a fact-intensive process. Ultimately, a court will need to look at the issue to provide more guidance on how copyright interfaces with individual tweets, compilations of tweets, and those linking to tweets.

---

To order this newsletter, call: 1-877-256-2472

On the Web at: www.ljnonline.com

January 2010