Social Media In and Out of the Courtroom

Presented by Dixon Robertson

Introduction

Social Media vs. Social Networking

Social media are a diverse mix of applications, platforms, and websites that let users interact with one another. They include

- Communicating by blogging, microblogging, geolocation applications, and events and meetings. Examples include WordPress, Twitter, Foursquare and Yelp.
- Sharing music, photographs, videos, and other files. Examples are Pandora, Flickr, Picasa, YouTube, and SlideShare.
- Collaborating and tagging, like wikis, Delicious, Digg and PBworks.

Social networking may include other social media features, but focuses on building relationships between people with shared interests. Think virtual high school reunion. Except you can be pickier about your friends, without seeming rude. And you don't have to listen to opinions of folks you never liked anyway.

Brief history of social networking

- Classmates.com: 1995. Originally designed to locate classmates from kindergarten through college. Acquired by United Online in 2004. Now part of Memory Lane and basically a fee-based source of nostalgia content.
- Friendster: 2002. Closest analog to present-day Facebook, used for maintaining contacts and sharing online content. Earlier this year shut down most traditional social networking functions and is transforming into a gaming site.
- LinkedIn: Launched in May 2003. IPO in May 2011. Currently claims over 100 million registered users. Facebook for professionals.
- Myspace: Launched August 2003 and acquired in 2005 by News Corporation for $580M. By 2006 was most popular social networking site in the US, but Facebook gained the lead in 2008. After several redesigns and attempts to redefine itself, Myspace has lost most of its users and employees. News Corporation sold its stake earlier this year for around $35M.
- Facebook: Launched for Harvard students only in late 2003; expanded to other colleges and high schools for the next three years. In September 2006 opened to anyone over 13 with an email address. Currently claims over 500 million users worldwide.
- YouTube: Video sharing launched in 2005. Acquired by Google in 2006.
- Twitter: Launched July 2006; currently has 200M users. Users post "tweets" limited to 140 characters. Sort of a private news and gossip service from contributors you "follow."

Copyright 2011 William Dixon Robertson III

Focus for today is social networking sites, principally Facebook.

Obtaining Online Content

Parties, fact witnesses, experts, jurors. And, of course, clients. Almost everyone has digital footprints. Tracking them down entails three stages: Search, collection, and preservation.

WARNING!

You can't "pretext" a Facebook member (or any other social networker) by concealing or misrepresenting that you are a lawyer. Check out these Rules of Professional Conduct (S.C. Sup. Ct. R. 407):

- Rule 4.1: A lawyer shall not make false material statements to a third person.
- Rule 4.2: A lawyer shall not communicate with a person represented by counsel.
- Rule 4.3: A lawyer shall not misrepresent her role to an unrepresented party or pretend to be disinterested, and must correct any misunderstanding as to these issues.
- Rule 5.3: A lawyer is responsible for the conduct of a non-lawyer assistant and must make reasonable efforts to ensure the person's conduct is compatible with the lawyer's professional obligations.
- Rule 8.4(a): A lawyer must not violate the Rules through the acts of another.
- Rule 8.4(d): A lawyer shall not engage in conduct involving dishonesty, fraud, deceit, or misrepresentation.

So, don't get cute or clever trying to get around privacy restrictions on any social networking site.

Search

Finding information online is easy and essential. Typically there are three ways to do this.

First, use a traditional search engine like Google, Yahoo! Search, or Bing. Search for full name in quotation marks, and for nicknames. Remember that Mark Zuckerberg doesn't like Larry Page, so Facebook blocks Google's search robots.

Second, visit the major social networking sites and use the search tools there. At a minimum go to Facebook and LinkedIn. If you think your subject has some tech sophistication, search Twitter and Technorati. If you suspect there may be photos or video out there, go to YouTube, Flickr, Picasa, and Vimeo.

Third, consider using a paid service. Spokeo is cheap--$15 for three months. You can search by name, email address, telephone number or username. Do all four. The results are astounding. You may find ebay purchases, blogs, social network accounts, music preferences, and other profile information.

Copyright 2011 William Dixon Robertson III

Collect

Your search reveals that the witness has a Facebook account. Now what? Nothing prevents you from viewing his public pages on the site. If, like most of us, he has left the default privacy settings alone, you will see a lot. If he has restricted access, though, revisit the "Warning" section above.

For public content, though, it's harvest time. In Facebook you can download photographs. You can use the "Print Screen" function as a poor man's screen capture. You can use Adobe Acrobat or Nuance PDF Create to save the page in pdf format. And those options may be all you need, if you don't expect—or care about—any authentication issues at trial. For a few dollars more, use a special screen capture tool like TechSmith Snagit or Ambrosia Software's Snapz Pro (Mac only).

Preserve

If you expect a challenge to the authenticity of the content, you must take additional steps to document the capture and "seal" the digital record. This means proving the sites IP address; and then freezing the image and other digital records to rule out any tampering with the screenshot. At least one writer has suggested that lawyers can do this. I'm not so brave.

There are at least two commercial products available that take care of this for you. One is NextPoint Cloud Preservation, an online service for creating defensible archival copies of websites. Pricing starts at $15 per month and rises quickly as the number of sites and the volume of storage increases. The other is AbsoluteProof WebSeal, by Surety, LLC. According to its website, "AbsoluteProof® WebSeal™ is the market's first Web-evidence collection, integrity preservation, and authenticity service, designed to support the global increase in Web-related litigation and investigation activities." Pricing information is available through email with the publisher.

Finally, think about hiring an e-discovery expert to collect the content and to authenticate it for admissibility. You don't want to risk becoming a witness in your client's case.

Facebook and Discovery

Subpoenas

Unless you are the government, you can only subpoena "basic subscriber data" from social networking site, including Facebook. Basic data includes the email address associated with the account; the date the account was created; recent logins; and, if provided by the subscriber, the mobile telephone number registered with the account. This isn't Facebook being unreasonable. It's mandated by the federal Stored Communications Act, 18 U.S.C. §§2701-2711. To read a wonderful article explaining why, check out O.S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It,* 72 Geo. Washington L. Rev. 1 (August 2004), available for download here. Facebook policy on civil subpoenas can be found here and here. Note that Facebook doesn't preserve content deleted by a subscriber, without a request from law enforcement.

Copyright 2011 William Dixon Robertson III

Interrogatories and Document Requests

About a year and a half ago, a Lowcountry judge ordered plaintiffs in an injury suit to:

> produce documents containing the following information from any Facebook or MySpace accounts, either in tangible or electronic form: (a) all Profile pages; (b) all Wall Postings, including status updates and comments from or to the Plaintiff; (c) all photographs depicting the Plaintiffs, including all mobile uploads and photographs in which the Plaintiffs are "tagged;" and (d) all information reflecting the "fan pages" and groups in which Plaintiffs are members. Such production shall include all documents/ information placed or reflected on the site accounts from the date of the accident through the present ….

Defendant offered no predicate for the discoverability of this information, besides the general assertion that people post pictures on Myspace and some of those pictures might show plaintiffs enjoying life after the defendant maimed them. Other jurisdictions take a more nuanced view of social network discovery.

The party answering discovery, or her lawyer, must identify documents responsive to a request. Suppose a defendant asks us for all photographs of our injured client engaging in outdoor activities. We must tell the client to look for those pictures; we must review them, if they exist; and we must either produce them or claim some privilege against disclosure. This initial obligation for the parties and counsel to determine relevancy is implicit in our discovery rules. If we respond to the request that no such documents exist, the inquiry doesn't necessarily end. Defense counsel will independently search for pictures, including online. She may subpoena third parties to produce them. If her investigation turns up nothing, she can't go to the court with an unsubstantiated suspicion and say, "Look, Judge, they say there are no pictures; I can't find any myself; and none of the plaintiff's family and friends have produced anything responsive to my subpoena. But I just don't believe all that. Please issue an order compelling plaintiff to produce those pictures." Well, she might, but she won't get far and she won't look too good. On the other hand, if she finds pictures that are responsive to her request, then she will ask the court to compel our client to produce additional documents. The judge should grant that motion. And we will look bad, because the judge will think we deliberately hid photos we thought would hurt our case.

So, generally speaking, there are two ingredients for a successful motion to compel: first, a properly drawn request for documents, or interrogatory; and second, some basis for believing responsive documents or information are being withheld—a factual predicate for the motion to compel.

There is, of course, a third approach. We can respond by saying those pictures, if they exist, are none of your business. Or, if they are your business, they are privileged somehow. When we do that we relieve defense counsel of her obligation to give the court a reason why she doesn't believe we are responding properly. In fact, the objection admits there may be documents responsive to the request. In each case where a court has ordered disclosure of social network content, there has either been an implicit admission that responsive material exists; or independent evidence that the response is not complete.

Copyright 2011 William Dixon Robertson III

Mackelprang

The earliest case I found dealing with production of Myspace content was *Mackelprang v. Fidelity National Title*, 2007 WL 119149 (D. Nev. 2007). Plaintiff was married and had six children. She attempted suicide in her office, after being coerced into having sex with two of her supervisors over a period of several months. She never returned to work. Nearly a year later she apparently created a Myspace account where she described herself as single and childless. The account was accessed only a few times and was abandoned about six weeks after it was created. Five months after opening the first account she created another, where her profile claimed she was married and loved all of her six children. The second account, like the first, was sparsely used. When defendant learned of the accounts it served a subpoena on Myspace for the entire content of both accounts. Myspace responded with basic subscriber data but refused to disclose any content absent Mackelprang's consent. When Mackelprang refused to execute a consent form defendant moved to compel production of all private message traffic and other content from the two accounts.

In its discussion the district court noted:

> Defendant has no information regarding the identities of the persons with whom Plaintiff has exchanged email messages or what the subject matter or content of those email messages are. Defendant raises a number of issues, however, regarding the type of information that might be contained I the messages that would be relevant to the issues in this case … [but] at this time, it has nothing more than suspicion or speculation as to what information might be contained in the private messages.

Mackelprang, id. at *2. Defendant whined that limiting production to relevant material only would allow plaintiff's counsel to determine discoverabilty. The court answered that complaint succinctly:

> The defendants are correct that an interested party cannot be the "final arbiter" of relevance. But counsel for the producing party is the judge of relevance in the first interest. Discovery in our adversarial system is based on a good faith response to demands for production by an attorney constrained by the Federal Rules and by ethical obligations. Where the parties disagree as to the contours of relevance in connection with particular discovery demands, they present their dispute to the court, as the parties have done here. When a party can demonstrate that an adversary may be wrongfully withholding relevant information, it can seek relief; in this case the defendants have made no such showing.

Id. at *8. Result: motion denied, without prejudice to defendant's right to serve "properly limited requests for production of *relevant* email communications." *Id*. (emphasis in original).

Leduc

Chronologically, the next case comes from Ontario, Canada: *Leduc v. Roman*, 2009 CanLII 6838 (Ont. Sup. Ct. 2009). In 1974 Roman injured Leduc in a car crash. Leduc sued in 2006. Among his damages was loss of enjoyment, including his inability to engage in sporting activities. In 2008 defendant found Leduc's Facebook profile. Because of the privacy settings, only Leduc's name and a "head shot" photo

Copyright 2011 William Dixon Robertson III

were visible. Under Canadian procedure, parties must swear in an affidavit that all relevant documents responsive to a request have been produced. Leduc submitted an unsworn affidavit of documents that contained no reference to Facebook content. Roman moved for an order to preserve all Leduc's Facebook content; to produce that content in its entirety; and for a new affidavit of documents.

The motion was referred to a master. He found that Facebook profile pages were "documents" within the plaintiff's control and ordered Leduc to copy and preserve all Facebook content. He also held that Roman had offered nothing to suggest there were relevant materials on the private profile pages, beyond the mere existence of the account, and thus refused to order production of the content. Roman appealed to the Superior Court. That court agreed with much of the master's ruling:

> Master Dash did not err in his articulation of the law regarding motions under Rule 30.06. He acknowledged that Mr. Leduc had an obligation to produce all relevant documents in his possession, including any information posted on his private Facebook profile demonstrating activities and enjoyment of life, "even if it is contrary to his interests in this action". Master Dash also correctly noted that where, on a Rule 30.06 motion, the defendant contends that the plaintiff has not met his obligation to produce relevant documents, then the defendant must provide some evidence that the plaintiff has relevant materials in his possession or control.

Id. at 4.The court parted with the master, though, and found "from the social networking purpose of Facebook, and the applications it offers to users such as the posting of photographs, that users intend to take advantage of Facebook's applications to make personal information available to others." *Id*. at 7. He agreed that "mere proof of the existence of a Facebook profile does not entitle a party to gain access to all material placed on that site." *Id*. Rather than order production of the content, though, the judge allowed Ramon to cross-examine Leduc on the latter's affidavit of documents, to determine what kind of content he posted on the profile. If Leduc's answers suggested there may be relevant material in the profile, "production can be ordered of the relevant content." *Id*. at 8.

Romano

A defense favorite is the New York case of *Romano v. Steelcase*, 2010 NY Slip Op. 32645 (Suffolk Co. Sup. Ct. 2010). Romano fell off a chair manufactured by Steelcase and claimed to be homebound, in constant pain, and largely bedridden. On her public Facebook profile were pictures of her smiling, outdoors, and engaging in an "active lifestyle." *Id*., slip at 2. Defendants asked Romano questions about her Facebook and Myspace postings at her deposition, which she refused to answer. She also refused to provide consent for release of the content of her social networking profiles. Defendants' motion to compel that information was granted, largely because of the stark contrast between Romano's description of her condition and the photographic record in the public areas of Facebook and Myspace:

> [I]t appears that Plaintiff's public profile page on Facebook shows her smiling happily in a photograph outside the confines of her home despite her claim that she has sustained permanent injuries and is largely confined to her house and bed. In light of the fact that the public portions of Plaintiffs social networking sites contain material that is contrary

Copyright 2011 William Dixon Robertson III

> to her claims and deposition testimony, there is a reasonable likelihood that the private portions of her sites may contain further evidence such as information with regard to her activities and enjoyment of life, all of which are material and relevant to the defense of this action. Preventing Defendant from accessing to *[sic]* Plaintiffs private postings on Facebook and MySpace would be in direct contravention to the liberal disclosure policy in New York State.

Id., slip at 2-3.

McMillen

In *McMillen v. Hummingbird Speedway,* No. 113-2010 CD (Jefferson Co., Pa., Ct. of Comm. Pl.), McMillen sued the driver of a losing racecar who rear-ended him during the cool-down lap after the race ended. He claimed permanent disability and inability to enjoy many of life's pleasures as he did before the wreck. His public Facebook wall contained comments from friends about his fishing trips and travel (from his home in Pennsylvania) to the Daytona 500. When asked to provide login credentials for Facebook and Myspace, he acknowledged membership but claimed that his login information was confidential and thus protected by some "privilege." Although the court spilled six pages of toner in rejecting McMillen's claim, the result was never in doubt. Here is the money quote:

> Where there is an indication that a person's social network sites contain information relevant to the prosecution or defense of a lawsuit, therefore, and given *Koken's* admonition that the courts should allow litigants to utilize "all rational means for ascertaining the truth," 911 A.2d at 1027, and the law's general dispreference for the allowance of privileges, access to those sites should be freely granted.

Id., September 9, 2010, Order at 7.

McCann

McCann v. Harleysville Ins. Co. of N.Y., 78 A.D.3d 1524, 910 N.Y.S.2d 614 (4th Dept. 2010), though terse in its discussion, underscores the requirements for both specific requests for information and a factual predicate for an order to produce all content. McCann sued Harleysville to recover proceeds of UM/UIM insurance following a car wreck. Harleysville sought disclosure of all McCann's Facebook content. It apparently filed serial motions to compel, both of which were denied. Affirming, the Appellate Division noted the initial request was overly broad, and that the denial of the first motion to compel was without prejudice to service of narrower requests. As to the second motion, the Appellate Division cited Harleysville's failure "to establish a factual predicate with respect to the relevancy of the evidence [Facebook content]," and admonished against "fishing expeditions" (the court's words) into Facebook accounts "based on the mere hope of finding relevant evidence." *Id*., slip op. at 1.

Simply Storage

For an example of an evenhanded approach to social networking discovery, read *EEOC v. Simply Storage Mgt., LLC*, No. 1:09-CV-1223-WTL-DML (S.D. Ind.). It's a workplace sexual harassment case brought on behalf of two named individuals and a number of other women similarly situated. Simply Storage requested virtually all content posted by the two lead plaintiffs on Facebook and Myspace. EEOC

Copyright 2011 William Dixon Robertson III

requested a discovery conference to determine the limits of social networking discovery and the court issued a comprehensive order on May 11, 2010. Although it objected to the requests, EEOC acknowledged that some content was discoverable. It argued "that production should be limited to content that directly addresses or comments on matters alleged in the complaint." *Id*., May 11, 2010, Order at 5. Simply Storage insisted that, because these two women claimed emotional distress, all content was potentially relevant. The court laid down some general ground rules for disclosure, striking a balance between the defendant's legitimate need for information and the plaintiffs' privacy. And the reasoned approach by plaintiff's counsel, I believe, played no small part in the result.

So where does this leave us? First, understand that Facebook content is discoverable. Don't argue that it is privileged or "confidential." If the content is relevant to the claims or defenses in the case, or reasonably calculated to lead to the discovery of relevant evidence, it must be disclosed. And remember, by posting to Facebook your client has already disclosed to at least one third party, so I don't see what privilege might apply. Second, make the defense lawyer earn her money. She must ask you to identify specific discoverable content, and then to produce that content (and only that). Third, never surrender blanket consent for content or, worse, login credentials. Whatever defendant may need doesn't include the keys to the kingdom. Third, emphasize that defendant needs more than an unfounded suspicion—or the mere existence of an account—to gain access to your client's content. Facebook content may not be privileged or confidential, but it is (somewhat) private. Educate the judge on the absolute necessity of establishing a factual predicate for invading that privacy. Finally, be reasonable. In both cases I cited where the court ordered complete production of content, plaintiff's counsel staked out an absolutist position. Romano's lawyer refused to allow questioning about Facebook content, notwithstanding the public—and very embarrassing—information the defense already had from there. In *McMillen*, counsel asserted a vague theory of privilege without support in Pennsylvania's case law.

How to Preserve Facebook Content

Facebook has a tool to collect and save all the content posted to a subscriber's account. To use it, from the home page click on "Account," then "Download a copy of your Facebook data." Click the green "Download" button, and then click the one that appears in the "Request my Download" box. You will see a box that tells you to expect an email when the file is ready to be downloaded. When the email arrives, click on the link and save the file. It's probably a best practice to do this for your clients.

What shall we tell the clients?

Here's another quote from the *Leduc* case, in February 2009:

> Given the pervasive use of Facebook and the large volume of photographs typically posted on Facebook sites, it is now incumbent on a party's counsel to explain to the client, in appropriate cases, that documents posted on the party's Facebook profile may be relevant to allegations made in the pleadings.

Leduc, ante at 7. A couple of years ago I sent letters to my clients warning them that nothing they post to the Internet is private. Here's what else I told them:

Copyright 2011 William Dixon Robertson III

> Review your online postings. Use Google, Bing, or Yahoo!Search on yourself. Is there anything that would embarrass you if, say, your parents, or your children, read it? What if a jury saw it, right after you testified in your legal case? If you find offensive or compromising material, can you edit it? If you can't remove it, tell me about it. Please don't let the first time I learn about it be at your deposition or, worse, at trial.
>
> The Internet is a fabulous tool. I don't know what we did before Google or Mapquest. I blog. I leave comments on news and other public interest sites. I post to different special interest lists. I even have a Facebook page. I'm not suggesting that you stop using the internet to express yourself. Just remember that very little of what you post to the web will ever go away, and use some discretion when you post.

Today I am not sure my advice—to edit or remove embarrassing content—was sound. Parties must preserve evidence during the time leading up to suit if she "reasonably should know that the evidence may be relevant to anticipated litigation." 32B Am.Jur.2d Evidence §2111 (2007). I remember some lively exchanges with my former law partners about what obligation we owed to counsel clients about internet use. There were three positions: tell 'em to scrub, make 'em preserve, and don't say anything. I read a blog post recently commenting that defense counsel monitor claimants' internet posts from early in their cases. I would expect insurance adjusters to begin monitoring the internet use of accident victims as soon as they learn their names, as a matter of routine. That means spring cleaning may attract notice from the defense, and the scrub advice may invite accusations of spoliation. But we need to tell our clients something.

In a presentation to the California Bar last year, lawyer Dana Shultz listed this advice for our clients:

- Modify all passwords to prevent a false profile or information
- Review "friends" lists
- Ask for attorney review of websites, including social media profiles
- Don't vent in social media
- Ask for attorney review of children's social media sites
- "Don't post anything you would not want children or judge to see"
- "If possible, stop!"

Your intake process should ask for all your client's social media accounts. Not login credentials, but enough for you to review the public information posted on them. Someone needs to advise on privacy settings—I just don't know if that is a lawyer's function.

On the Offensive

Things to do:

- Make social media discovery part of your overall discovery in all your cases.

Copyright 2011 William Dixon Robertson III

- Most of us send preservation letters to potential defendants warning against destroying documents or other evidence. Particularly when suing individuals, include social media (yes, media, not just social networking) in your preservation letter.
- Make sure your definition of "documents" speaks generally to electronically stored information (as defined in FRCP R. 34(a)) and specifically to ESI the defendant may have posted to social media: Facebook, "tweets," blogs, link- or file-sharing sites.
- Ask about social media in depositions. Remember you may need to compel production of Facebook content: don't forget to establish a factual predicate for that production.
- Send requests for admission if you anticipate challenges to the authenticity of social networking content.

Businesses use social media, too. Ask the same questions. And try these as well:

- Does the company have a social media policy?
- How does the company use social media? Marketing? Research? Customer service?
- Are there company social media sites?
- Does the company monitor social media? How?
- Who can post on behalf of the company?

Don't forget there are "private" social media. Ask about these things:

- SharePoint, a Microsoft product, has become ubiquitous in the business community. SharePoint features include My Pages, an internal profile page; blogs; wikis; and document repositories.
- Microsoft Office Groove is still around. Groove creates a group workspace for sharing documents, chat, and other information, accessible online by group members.
- Companies may have custom solutions with "internal" social networking functions. Or they may use open-source applications.

Online Content as Evidence

Social media evidence is just electronically stored information from a different source than the defendant's files. The same evidence rules apply as for any other evidence. You must still preserve the evidence (see above). And you have to remember the basics.

Lorraine v. Markel American Ins. Co., 241 F.R.D. 534 (D. Md. 2007), is a must read for anyone facing evidentiary challenges to social media content. In *Lorraine*, Magistrate Judge Paul W. Grimm denied cross-motions for summary judgment supported by dozens of email messages, on the ground that neither party had made any attempt to authenticate the communications or otherwise advise the court of the basis for their admissibility. The judge was clearly frustrated by counsel's failure to provide him with admissible evidence supporting their motions, and apparently peeved at the absence of clear guidance in existing case law for admission of electronically stored information under the Federal Rules of Evidence. Judge Grimm's 51-page order is a handbook for proffering ESI. In it he discusses different kinds of ESI, including website content, and the different bases for its admission. His decision is replete

Copyright 2011 William Dixon Robertson III

with citation to cases and evidentiary treatises. It is a simple matter to take *Lorraine* as a starting point to develop an "admissibility checklist" for all kinds of ESI.

Relevance

In most cases this should not be difficult to establish. Relevancy criteria aren't any different for social media content than for other evidence.

Authenticity

Authentication is a little different for social networking content, but many of the same considerations apply. There are two levels of authentication. First, does the printout actually represent what appeared on the website on the particular day it was captured? And second, did the substance of the post really come from the purported author? The second question can get more complicated.

There are different ways to skin the authentication cat.

- Acknowledgment or Stipulation. This is the easiest way to authenticate. Ask the author about the content in his deposition. Send him an interrogatory. Send requests for admissions.
- Authentication by Website. You won't get this from Facebook—its FAQ's state that only the account owner needs to testify about authenticity. But if content is produced pursuant to a subpoena accompanied by the account owner's consent, it may be self-authenticating, at least in district court.
- Third Party Testimony, SCRE R. 901(b)(1). Can the person who found the content testify, or give an affidavit, establishing what it is? Or do you need a computer forensics expert? See the section above on preserving content as evidence.

Hearsay

What is the purpose of the evidence? If not offered for its truth, it's not hearsay.

Offer it as a prior statement, SCRE, R. 801(d)(1)), or an admission of a party, R. 801(d)(2).

Invoke an exception to the hearsay rule.

- Present sense impression, R. 803(1): Tweets, Foursquare or Yelp check-ins
- Then Existing Mental, Emotional, or Physical Condition, R. 803(2)
- Recorded Recollection, R. 803(5)
- Reputation as to Character, R. 803(21)

Best Evidence

Should be no obstacle, provided authenticity is solid. Rule1001(3) states that "If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original'."

Probative value vs. Prejudicial Effect

As with any other evidence, Rule 403 allows the trial judge to exclude information which is unquestionably relevant. For social media evidence this issue arises most commonly in two

Copyright 2011 William Dixon Robertson III

circumstances: Where the evidence contains offensive or derogatory language that could provoke an emotional response; and where the court is concerned about the reliability or accuracy of the information contained within the electronic evidence.

Evidence Issues

The contrasting approaches different courts take to authentication are illustrated by two recent criminal cases, from Maryland and Florida. In the Florida case, a detective with Miami-Dade's sex crimes unit entered an AOL chatroom using an alias. He pretended to offer his fictional 14-year-old daughter for sex to Keith Lanzon. During the chat he set up a meeting with Lanzon and the fictional teenager. Lanzon was arrested when he showed up for the meet. *United States v. Lanzon*, 639 F.3d 1293 (11th Cir. 2011). At trial the detective testified how he preserved the AOL chat transcript:

> Detective Clifton saved these online conversations by copying the instant message communications and pasting them into a Microsoft Word document. He then saved the Word document to a floppy disc, where the conversations could be printed in hard copy form as transcripts. Detective Clifton did not save any of the instant message conversations in their original format to his computer's hard drive, but he compared the actual instant message "chat screens" to the word processing document he had created to ensure that they exactly matched and that he had accurately recorded the conversations in their entirety.

Id., slip op. at 4. Lanzon objected to the introduction of the chat "transcript" and challenged the evidence on appeal. Among his complaints was the claim that, by transferring the messages to Microsoft Word and then deleting the original, Clifton prevented Lanzon from determining (through hash values or digital "seals") if anyone had tampered with or altered them. Lanzon claimed this process was fatal to authentication under FRE rule 901(a). The Eleventh Circuit affirmed, holding (without a lot of discussion) that Clifton's testimony sufficiently authenticated the transcript under Rule 901(b)(1).

Maryland's story has a different ending. Antoine "Boozy" Griffin was charged with murder after chasing a man into the ladies' room of a nightclub and shooting him seven times. His first trial ended in a mistrial. At the second trial, a key witness changed his testimony favorably to the prosecution. He claimed he had been threatened by the accused's girlfriend, Jessica Barber. To bolster his testimony, the state offered a heavily redacted printout of a Myspace page. The page identified its owner by the nickname "Sistasouljah." The profile gave her hometown as Port Deposit, from where Barber hailed; and her birthday, which was the same as Barber's. A police officer offered the following testimony to authenticate the exhibit:

> [DEFENSE COUNSEL]: How do you know that this is her web page? . . .
>
> [SGT. COOK]: Through the photograph of her and Boozy on the front, through the reference to Boozy, to the reference of the children, and to her birth date indicated on the form.
>
> [DEFENSE COUNSEL]: How do you know she sent it?

Copyright 2011 William Dixon Robertson III

> [SGT. COOK]: I can't say that.
>
> Sergeant Cook acknowledged that he could not determine when any particular posting was made. But, he indicated that he visited the Web site on December 5, 2006, the date that appeared on the printout.
>
> The court ruled that it would admit a single, redacted page from the MySpace printout, containing only the photo next to a description of the page creator as a 23 year-old female from Fort Deposit, and a portion of the blurb, stating: "FREE BOOZY! ! ! ! JUST REMEMBER SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!"

Griffin v. State, 192 Md. App. 518, 995 A.2d 791, slip at 6-7 (Ct. Sp. App. 2010) *(Griffin I)*. The state offered the exhibit under Rule 901(b)(4), claiming the photo, nickname, birthday and reference to the children provided sufficient "distinguishing characteristics" for authentication. The Court of Special Appeals spent a lot of time reviewing authorities, including *Lorraine, ante*; and discussing the difficulties in authenticating evidence which was created anonymously. Ultimately, though, it deferred to the trial judge's discretion to accept the circumstantial authentication evidence provided by the officer's testimony. The decision spawned a multitude of blog posts, many with the theme "Maryland Makes it Easy to Authenticate Myspace Pages."

The state's high court took a less sanguine view of social media evidence. In *Griffin v. State*, 2011 WL 1586683 (Maryland Court of Appeals 2011) (*Griffin II*), the Court of Appeals reversed Boozy's conviction. The analysis in Griffin II begins with comments like "[a]nyone can create a MySpace profile," slip op. at 7, and that "anyone can create a fictitious account and masquerade under another person's name or gain access to another's account by obtaining the user's username and password," *id* at 8. Clearly the Court of Appeals was more concerned with the second phase of authentication: Had Jessica Barber really posted "Snitches get stitches?" Citing *Lorraine* again, the court criticized the state for what it had failed to do: It never questioned the girlfriend about the web post; never examined the girlfriend's computer; and never contacted Myspace for information about the Sistasouljah account. A dissenting judge accused the majority of "technological heebie-jeebies" and suggested that authentication concerns, once the proponent has made a prima facie case, go to the weight of the evidence and not to its admissibility.

What can we learn from *Lanzon* and *Griffin*? In *Lorraine*, Judge Grimm notes that it's better to be lucky than to be good. *Lorraine, ante* at 559. The prosecution in *Lanzon* caught a break, while the district attorney in *Griffin* did not. As Judge Grimm teaches, we need to plan for those times when we aren't lucky. If Sergeant Cook had used the considerable tools available to law enforcement to contact Myspace; if the state had recalled Barber at trial to ask about Sistasouljah; if the prosecution had spent a little money to forensically examine Barber's personal computer, Boozy might not be waiting for his third trial. Heed Judge Grimm's advice:

> [C]ounsel would be wise not to test their luck unnecessarily. If it is critical to the success of your case to admit into evidence computer stored records, it would be prudent to

Copyright 2011 William Dixon Robertson III

> plan to authenticate the record by the most rigorous standard that may be applied. If less is required, then luck was with you.

Id.

Jurors Behaving Badly

Jury use of social media undermines due process and usually constitutes misconduct. It falls into four broad categories:

- Tweeting or posting information about the trial
- Independently researching the law or facts in a case on the Internet
- Contacting parties, lawyers, witnesses or judges through social media
- Premature deliberation/broadcasting deliberations

Strutin, Social Media Misbehavior by Jurors Afflicts Trial Process, N.Y.L.J., March 15, 2011.

At least two organizations have proposed cautionary instructions for prospective jurors:

Judicial Conference of the United States Proposed Model Jury Instructions, The Use of Electronic Technology to Conduct Research on, or Communicate about a Case (December 2009)

American College of Trial Lawyers, Jury Instructions Cautioning Against Use of the Internet and Social Networking (September 2010)

Social Media Policy

Does your firm have a social media policy? Here is a site with dozens of samples, templates and go-bys. Now you have no excuse.

Copyright 2011 William Dixon Robertson III