The Facebook Grenade: Mining Social Media For Maximum Effect

By Zach Matthews
Swift Currie McGhee & Hiers
Atlanta

Imagine this scenario: you're defending a personal injury case against a plaintiff with a pre-existing history of injury and exaggerated claims. You strongly suspect your plaintiff is fibbing, and so you decide to check his Facebook profile and other social media postings. Alas! The plaintiff's lawyer has gotten there first with good advice, and the plaintiff has set all his social media accounts to private. What is your next move? Do you throw in the towel and begin bargaining based solely on plaintiff's sparse medical history? Even if you were successful in recovering damaging social media postings, how would you use them most effectively?

This common situation arises in many – possibly the majority – of personal injury defense cases these days. Properly handled, social media postings by or about the plaintiff can explode like a grenade, sinking a plaintiff's case and resulting in massively decreased settlement demands or a great trial result. Improperly handled, that grenade can explode in your own face, potentially leading to sanctions or even ethical complaints against you, the defense lawyer. The following are best practices to (ethically) get the absolute most out of your social media investigation and then use those gleanings for maximum effect.

First and foremost, you as the defense lawyer need to be aware of the playing field. The major social media websites these days are Facebook (facebook.com); Twitter (twitter.com); Instagram (instagram.com, but primarily available through an app); and LinkedIn (linkedin.com), which is often useful in lost income cases. Depending on the type of case, you may also find yourself trolling some of the darker corners of the web, including Craigslist (craigslist.com), a classifieds website; and Backpage (backpage.com), a classifieds website that spun off of Craigslist a few years ago and is now dedicated exclusively to human sex trafficking and other such offers. (Note: Backpage.com is decidedly not safe for work under ordinary circumstances.) Occasionally you will still encounter a plaintiff with an older social media profile on MySpace (myspace.com); or potentially on new up and coming sites like Reddit (reddit.com); Tindr (Tindr.com), a dating website; or even on fantasy sports pages like DraftKings (draftkings.com).

Identifying the Plaintiff Online

The first issue you are likely to encounter is *locating* the plaintiff's social media profiles. While it may be tempting to simply send an interrogatory request demanding that the plaintiff reveal his or her own account names, this tactic can be counterproductive. The best practice is to hold off on pursuing the social media angle in the first round of discovery while doing your own investigation and preservation of evidence *first*. (That way you'll be in position to know whether a plaintiff is hiding or deleting certain posts in response to your first round of interrogatory requests).

Certain factors are always important in a social media investigation: first, knowing the plaintiff's name and nickname(s), as well as his or her location. If you're lucky, this will be enough information to turn up the plaintiff's profile in a simple Google search or a search within Facebook's contained environment. However, because Facebook's own internal search algorithms leave much to be desired, don't give up if you can't find your plaintiff on the first pass, especially if they have a common name like "Tom Jones" or "Sarah Smith," which may trigger a multitude of Google hits. It is the rare plaintiff indeed who has no social media presence whatsoever these days.

Phone numbers are also valuable search information, which can often lead to the most important marker of a particular plaintiff online: his or her favorite "handle." Facebook accounts are actually linked to individual's phone numbers. In a little-known trick, you can search via the Facebook app on a phone or tablet for a profile using only the plaintiff's phone number. This trick doesn't work on the

Continued on page 48

Continued from page 18

Facebook internet site; only on the phone/tablet app. Plaintiffs will often reveal phone numbers without a second thought in their initial round of discovery responses, but they may balk at revealing their Facebook pages. Meanwhile, during your initial investigation you really do not want them to be thinking about social media at all.

"Handles" go back to the early days of CB radio, but they live on in the form of Facebook, Twitter, and other social media account names. These days very few individuals are able to secure their own legal name as an account name, although some early adopters (including myself) will have moved quickly and grabbed those accounts. Facebook uses the account name in the form of a directory identifier, which you can use, via your web browser's URL bar, to locate a plaintiff's profile page. For example, my account name on Facebook is "ZachMatthews" so type "www.facebook.com/ZachMatthews" in a web browser's URL bar and simply push enter to pull up my personal Facebook profile. Here's the thing about handles: people tend to re-use them. It is extremely common for a person to have the same handle across a multitude of social media platforms.

Thus, your search might play out as follows: after an initially fruitless attempt to locate "Sally Smith" via a Google search, which turns up thousands of results, you decide to serve interrogatory requests asking the plaintiff to identify, among other things, her cell phone number. Upon receipt of her responses, you plug the number into the Facebook app on your phone, thereby identifying her personal Facebook profile. Now that you know which "Sally Smith" Facebook account is hers, you can pick it out of the multitude of Google hits, and pull up her profile in a web browser so that you can look at the URL at the top of your browser page. For this example, turns out Plaintiff Smith is a rabid Tennessee Volunteers fan, and thus has chosen "SallyVol4Evr" as her Facebook profile login; that means the corresponding URL is "facebook.com/SallyVol4Evr". You return to Google, and enter "SallyVol4Evr" in the search block (in quotes to limit the hits to only that particular sequence of letters and numbers), thus revealing that Sally has also chosen the same handle on Pinterest (a social media sharing site that is typically of limited use from an investigation standpoint) and also, much more interestingly, on Instagram. Sally's love for the Tennessee Volunteers turns out to be the keys to her online kingdom, and now you can begin your investigation in earnest.

Mining the Resource

Facebook is like catnip for many plaintiffs (and indeed non-plaintiffs): they cannot resist the urge to share their innermost thoughts and activities with the world. Facebook also has questionable privacy settings, an overly intricate web interface, and a well-published corporate philosophy to "move fast and break things" in the words of founder Mark Zuckerberg. Simply put, it is not in Facebook's best business interests to make privacy a priority, and thus the default mode of operation is usually one of public sharing. As a result, privacy settings are rarely as straightforward or robust as a privacy-conscious individual might wish.

One important caveat which needs to be addressed: there is a growing body of law nationwide in which courts and ethical boards have ruled that "friending" a person on Facebook is a form of impermissible contact with a represented party. *See, e.g.,* Opinion 2009-02, Philadelphia Bar Association Professional Guidance Committee (March 2009). As defense lawyers, our priority should *always* be to lie in the weeds during social media investigations. Remember, for example, that LinkedIn allows its users to see the most recent visitors to their pages – if you click a plaintiff's LinkedIn page while you yourself are logged on, the plaintiff will be able to tell you have viewed his profile, and will be reminded to watch his actions. (To view a LinkedIn profile safely, enter the browser's 'Incognito' mode, which will disable tracking of your computer, *before* navigating to a plaintiff's page).

You will often find that plaintiffs, acting on the advice of their attorneys, will already have set, for example, their most recent Facebook posts to "Only Friends" (thus preventing you from seeing the newer posts, even if you can view the profile page). However, frequently a subject will have increased his or her privacy settings only on the browser version of Facebook, and not on items posted from the Facebook phone/tablet app. Oftentimes they thus inadvertently continue sharing a trickle of their postings with the outside world. Of course, in many situations a plaintiff will stop posting altogether ... once they hire a lawyer. Even where a plaintiff has locked down all new content, he or she may forget to secure the *old* postings. A plaintiff's social media posts made in the interim period between an incident and their retention of counsel can be very useful indeed.

The cardinal rule of mining a plaintiff's Facebook page is to save everything. The best practice is to print a full-color copy of everything you can see on the profile as soon as you first access it. Save the highest resolution copies of Plaintiff's photos that you can. You never know when a plaintiff will decide to make his or her postings unavailable – and you may not win a discovery battle to force them to disgorge materials you only vaguely recollect seeing. For this reason, social media review should also be one of your first steps in investigating any new claim referred to your desk. In addition to printing a paper copy, you can also use the screen capture feature of any computer to save screen-

shots from a plaintiff's profile page with helpful comments and time-stamps. These screen clippings can be very useful when it becomes time to prove up a plaintiff's inconsistent statements on the stand. Jurors are familiar with a Facebook interface and will know the photos were both authentic and secured from Facebook, which only the plaintiff could have posted. Be sure to save and/or stamp any retained materials with the date and time you yourself accessed them, as this may also become important later.

This advice also goes for video, which, of course, cannot be printed. Although Facebook is coded to prevent outright capture of posted videos to save locally, there is a workaround: once you locate the video you wish to save in a web browser, enter the mobile version of Facebook by changing the "www" to "m" (for mobile). Thus, instead of "www.facebook.com/...", your URL would become "m.facebook.com/..." (with the ellipses representing the remaining gibberish identifying the particular video's page). Change *only* the "www" to "m" then push enter. Now in mobile mode, albeit accessed through a regular web browser, you can push play to start the video, then pause to stop it. A paused Facebook video accessed in mobile mode can be saved: simply right-click the video and choose "Save as ..." to retain the full video file locally.

It is rarely possible to cherry pick only the relevant information in a first pass of social media investigation – you typically haven't deposed the plaintiff yet and may not yet know what he or she will claim to be unable to do. Thus, blanket retention is the rule of the day. Be sure to convey this in the clearest possible terms to any associate or staffer you charge with retaining the evidence.

What if a smart plaintiff has set her social media page to be entirely private? Don't give up. I once was involved in a trial in which the plaintiff lied on the stand about a certain disfiguring injury preventing him from ever wearing short sleeves again. Luckily, I had devoted the hours to mining not only his *own* Facebook profile, but also to identifying that particular plaintiff's closest friends' Facebook profiles as well as the plaintiff's favorite hang-out, a local restaurant, which also had a Facebook page. In meticulously reviewing those companion pages I identified photos of our plaintiff not only wearing short sleeves outdoors at a parade, but also actually giving a toast at a wedding, holding his "disfigured" arm up for all to see, in specific contradiction to his sworn testimony. His friends had not tagged him in these publicly-available images, and thus he did not know they were out there. At trial, this evidence was used during his

... there are additional legal tactics that act as the priming trigger on the Facebook grenade.

cross-examination for impeachment purposes (discussed in detail below), and the jury wound up awarding the plaintiff the exact figure, to the cent, which we had offered at mediation. The moral of this story is to keep banging away: use the plaintiff's friends list; use the friends list of known family members. Identify places the plaintiff likes to hang out and determine if that restaurant or CrossFit Box or roller rink has a website or Facebook profile. If you put in the time, in my experience, in roughly three cases out of five you will find something extremely valuable.

While Facebook will remain the main event for the foreseeable future, don't neglect Twitter, Instagram, or the open web. A privacy-conscious plaintiff may well forget just how many social media accounts he or she has made, and neglect to protect one. In back-to-back negligent security sexual assault cases, I was fortunate to locate the plaintiff's online profiles demonstrating that they were not, as they each claimed, regular college students. Instead, they were the kinds of individuals who would advertise on Backpage.com (the sex trafficking website). While their aliases were meaningless and changed by the day, in those cases their phone numbers could not change for business reasons. A phone number search thus revealed their postings. At the first mediation, plaintiff's counsel took one look through our manila envelope of printouts and we quickly reached a go-away value settlement. In the second mediation, plaintiff's counsel saw the same envelope, and simply said, "Here we go again." Once again his case collapsed.

Baiting the Trap

Just knowing about the plaintiff's (in some cases illicit) activities can be very helpful, but there are additional legal tactics that act as the priming trigger on the Facebook grenade. First and foremost, you want the plaintiff to exaggerate. Exaggeration is the key to impeachment, because even a "white lie" will allow you to prove up the inconsistency on the stand.

Start with your first round of Interrogatories. Ask detailed and probing questions about the kinds of things a plaintiff enjoyed doing before the accident, but can no longer enjoy as a result of it. Be careful about timeframes: don't give the plaintiff wiggle room by setting unnecessarily narrow parameters with your interrogatory or deposition questions, such as asking what the plaintiff can't do "today" or "in the immediate aftermath" of an incident. Make the questions broad enough for a plaintiff to get the gist without boxing yourself in; most are more than happy to tell you all about

their suffering as a way of trumping up their case.

Chances are you will discover useful material via social media that a plaintiff posted in the aftermath of the incident, which may be inconsistent with a plaintiff's sworn statements (for example if the plaintiff with the "debilitating neck injury" nevertheless was able to attend a season's worth of high school football games). However, if the plaintiff *later* had a surgery, which the plaintiff could claim had a bad outcome, that might give the plaintiff a plausible explanation for the increased level of activity after the accident (but before the surgery). You want the plaintiff to blame *all* of his or her suffering on the incident, and not on specifics such as a subsequent round of botched treatment, in order for the impact on the plaintiff's credibility to be as strong as possible. Word your requests carefully with this in mind. At the end of the day, whether or not the plaintiff really could do this or that is unimportant: whether the plaintiff is trustworthy is what matters. If the jurors believe a plaintiff is lying to them, they will penalize him or her heavily, every single time.

Sanctionable Conduct

Once you have the plaintiff's sworn responses to your Interrogatories regarding what he or she can no longer do as a result of the accident (being sure to also demand a Verification), and once you have used that information to secure her social media postings to your satisfaction, in the right case you may want to consider a second round of discovery requests now explicitly targeted at social media accounts and their content. This is where the chess match typically begins. In a best case scenario, upon receipt of your "follow-up" social media discovery requests, the plaintiff – in a panic – will begin deleting (rather than privatizing) harmful social media postings which you will already have retained, then will try to provide you with surreptitiously redacted materials. (Although foolish in the extreme, this is a surprisingly common occurrence).

Redacted social media postings received in response to your discovery requests can be cross-referenced against your saved materials, which will typically give you everything you need to prove up the intentional destruction of evidence. This of course is sanctionable conduct which can lead to, in a best case scenario, an outright dismissal of the plaintiff's entire case. *Chapman v. Auto Owners Ins. Co.*, 220 Ga. App. 539, 542, 469 S.E.2d 783, 785-86 (1996) (Dismissal appropriate where a party has maliciously destroyed relevant evidence with the sole purpose of precluding an adversary from examining that relevant evidence).

Alternatively, if you receive redacted responses, you might want to lay low and refrain from filing a motion for sanctions, instead saving the information you have retained for use at trial as impeachment material, and thus blindsiding the plaintiff with the posts the plaintiff thought he or she had safely hidden. If you are extremely lucky, the judge might even let you get away with questioning the plaintiff on his or her attempted destruction of evidence after the plaintiff's statements have been impeached on the stand, even though this is debatably relevant. Judges tend to take a dim view of perjury, and may rule that a perjurious plaintiff has opened the door to otherwise ancillary or dubiously relevant lines of questioning.

Discovery Battles

You are likely to draw objections to your first round of social media discovery requests, whenever you choose to send them. The law of social media discovery is not yet well-documented and thus plaintiff's lawyers often respond with knee-jerk objections, even to carefully crafted questions. Remember that statements the plaintiff makes about his or her physical condition (whether online or otherwise), as well as photographs depicting the plaintiff (again whether posted online or even taken by a private investigator), are relevant to the plaintiff's contentions of injury, and thus your social media requests will be reasonably calculated to lead to the discovery of admissible evidence. *Lindsey v. Turner*, 279 Ga. App. 595, 597, 631 S.E.2d 789, 791 (2006) ("evidence concerning a plaintiff's 'other' injuries may be admissible to show that the injuries currently at issue are not the result of the defendant's alleged negligence"); *Darwin v. Metro. Atlanta Rapid Transit Auth.*, 158 Ga. App. 635, 636, 281 S.E.2d 361, 363 (1981) (photographs and testimony of private investigator admissible for impeachment even where both the evidence and the investigator's existence was not disclosed in the pretrial order).

Recent Georgia federal cases have begun making it clear that the door is open to discovery of social media postings, which is already well established in other federal courts. "Generally, social networking site content is neither privileged nor protected by any right of privacy." *Jewell v. Aaron's, Inc.*, No. 1:12-CV-0563-AT, 2013 WL 3770837, at *3 (N.D. Ga. July 19, 2013); quoting *Davenport v. State Farm Mut. Auto. Ins. Co.*, No. 3:11-CV-632-J-JBT, 2012 WL 555759, at *1 (M.D. Fla. Feb. 21, 2012) ("Plaintiff will be ordered to produce [] all photographs added to any social networking site since the date of the subject accident that depict Plaintiff"). It is likely to be only a matter of time before similar decisions are reached in our Georgia state courts, making it clear that any social media posting by a plaintiff is fair game for discovery purposes.

Impeachment

The process of impeaching a witness with his or her prior inconsistent statements is well-understood. Most frequently, the defense lawyer will use the witness's deposition testimony after he or she takes a new position on the stand. "Turn with me in your deposition transcript," sometimes becomes a litany as a plaintiff's story crumbles around her. Of course, these are some of the most dramatic moments in any trial.

Social media impeachment is no different, but there are nuances for maximizing the impact with the plaintiff on the stand. Crucially, impeachment is the last bastion of so-called "trial by ambush," which is

otherwise highly disfavored. Defense attorneys are allowed to list "impeachment evidence" as an item in a pre-trial order without actually describing what the evidence will be. The rationale is of course that the plaintiff is expected to tell the truth on the stand; if they do not, on their own head be it. The Georgia Supreme Court has been abundantly clear on this issue: "It is impossible," the Justices held, "for counsel to know whether impeaching documents will even be relevant and admissible until the witnesses for the opposing party testify at trial, so there is no possible justification for requiring disclosure of such evidence in the pretrial order." *Ballard v. Meyers*, 275 Ga. 819, 820, 572 S.E.2d 572, 575 (2002). Thus, "the failure to list [an impeachment] document [is] not an intentional act of ambush, but an instance of adherence to applicable legal and professional concepts." *Id.*

Notably, this longstanding and clearly-articulated rule is in apparent conflict with the newest version of USCR 5.5(1)(b), which just went into effect on June 4, 2015: "Information withheld. When a party withholds information otherwise discoverable by claiming that the information is privileged or subject to protection as trial preparation material, the party shall: [] b. Describe the nature of the documents … ." This inartfully drafted language, which does not mention impeachment evidence but which is nevertheless in apparent conflict with decades of case law, may require a legal challenge (and revision) to solidify the retention of impeachment evidence in the near future. For the time being you as the defense lawyer should simply be aware of the new language so you can craft a response if plaintiff's counsel points to it when the evidence is deployed.

Typically, unless social media evidence has previously been disclosed (for example at mediation, discussed below), a plaintiff will never know what hit him until it is too late. The playbook for getting into social media evidence on the stand is straightforward.

First, during the plaintiff's cross-examination, rehash verbatim the plaintiff's earlier deposition testimony regarding their accident-related disabilities or alleged long-term injuries. A plaintiff might, for example, claim at deposition and then repeat on the stand that he or she can no longer enjoy spending time with children, or is not capable of strenuous physical activity.

Once the statement is made, courtroom technology like the Elmo projector can be used to display the contradictory social media posting (the plaintiff's post about riding a roller coaster, or video of he or she performing lawn work, etc.) directly to the jury. Invariably, the plaintiff's attorney will object, usually claiming hacking and citing the pretrial order, and the defense lawyer will need to be prepared to explain that all social media evidence was derived from *public* postings (not from inappropriate contact with a represented party), and was offered exclusively for impeachment purposes as allowed under explicit Georgia case law. *See, e.g., Ballard*, 275 Ga. at 822; *Minnick v. Lee*, 174 Ga. App. 182, 184, 329 S.E.2d 548, 550 (1985) (excluding impeachment evidence because it was not revealed beforehand "would be to elevate a pre-trial order to an almost unassailable position of conclusive sanctity even in the face of the statutory mandate that the object of all legal investigation is the discovery of truth").

This is where screenshots showing the pictures or materials came from the plaintiff's own postings are most helpful. A mere photo of the plaintiff may not provide the immediate context for both the jurors *and the court* to understand that the social media evidence is, most typically, the plaintiff's own admission against interest.

Social Mediation

Alternative dispute resolution or mediation is now the endgame for more than half of civil cases. Mediation also poses the greatest conundrum when it comes to use of social media gleanings. Imagine that you find yourself at mediation in possession of certain online postings – say a picture depicting the plaintiff chain-sawing a tree, despite his alleged back injuries – and you are not sure whether to use the evidence or not. The best advice is to avoid giving up the element of surprise unless the social media evidence is so overwhelming (as the Backpage.com evidence was in the negligent security sexual assault cases related above) that the evidence alone will absolutely shut down the case. If you find yourself closing in on five o'clock and still $100,000 apart, the temptation to show all your cards may become overwhelming. But if you reveal them, and the case does not settle, there is little doubt that the plaintiff will find a way to explain away the apparent inconsistency prior to trial.

Frequently, social media postings are only relevant to prove an inconsistency in the plaintiff's testimony. If the plaintiff is aware the harmful materials are out there, she may amend her testimony with nuanced affidavit testimony which meets the substance of her answers at deposition, but explains further, thereby eliminating the inconsistency altogether, and thus preventing introduction of the impeaching evidence on the stand. Harmful social media content is one of the defense lawyer's sharpest swords and should only be deployed when it has maximum potential impact.

Best Practices

Social media best practices can be summed up as follows: document everything, reveal as little as possible, and give the plaintiff enough rope to hang herself by asking careful questions about what she can (allegedly) no longer do. Properly deployed, the Facebook grenade has the power to change the outcome of cases, showing the jury the *real* truth of a plaintiff's situation, but only if the defense lawyer takes this aspect of investigation seriously and implements the playbook to perfection. ❖

Zach Matthews is a trial lawyer with Swift Currie McGhee & Hiers in Atlanta. He chairs GDLA's Young Lawyers Section and vice-chairs the Trucking Substantive Law Section.