POSTED AND TOASTED: BURNED BY SOCIAL MEDIA

By Joshua Burke

The actions of litigants—plaintiffs, defendants, even witnesses to accidents—are becoming increasingly easy to follow, thanks to social media. The successful use of social media tools is the next logical step in gathering information on parties to actions.

Until fairly recently, the best way to obtain information from social media sites was through image capture, printouts, or raw data archival of RSS feeds. The problem with all three of these methods is they fail to maintain a significant amount of the underlying information, or "metadata." In addition to the danger of missing potentially crucial metadata, printing social media sites to PDF or taking screen shots can cause additional problems, like incomplete or inaccurate data capture. Moreover, it is also impossible to capture dynamic material, such as video or sound recording. In the cases of *Griffin v. State*, 2010 WL 2105801 (Md.App. 2010) and *State v. Eleck*, 2011 WL 3278663 (Conn.App. 2011), social media evidence was excluded due to inadequate authentication of a printout from a Facebook or MySpace user's account.

Griffin v. State, *supra*, was an appeal to the Court of Appeals of Maryland of a second degree murder and first degree assault conviction. The prosecution's evidence hinged on an alleged printout of the defendant's girlfriend's MySpace profile page, which stated, "*JUST REMEMBER, SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!*" The MySpace printout was originally permitted at trial because it contained a photograph of the defendant's girlfriend, her birthdate, and identified the defendant as her boyfriend. However, the Court of Appeals ruled that the MySpace printout was not permissible evidence because the picture of the defendant's girlfriend, along with her birthdate and location, were not sufficient "distinctive characteristics" on a MySpace page to authenticate a printout, and that anyone other than the alleged owner of the page could have created it and posted the threatening comment. The Court of Appeals "recognize[d] that other courts, called upon to consider authentication of electronically stored information on social networking sites, have suggested greater scrutiny because of the heightened possibility for manipulation by other than the true user or poster." *Id*. The decision also stated that the Court was not suggesting that printouts of social networking sites should never be admitted as evidence, but aptly predicted that paths to properly authenticate a profile or posting printed from a social networking site will continue to develop as the efforts to evidentially utilize information from the sites increases.

State v. Eleck, *supra*, was a first degree assault case in which the defense sought to impeach a witness who was testifying for the prosecution. The witness' credibility was in question because she claimed that she had not spoken to the defendant in person, by telephone, or by computer since the alleged assault. However, the defense produced a printout allegedly showing an exchange of electronic messages between the defendant's Facebook account and the witness' account, dated after the alleged assault. The witness claimed that she did not post the messages, and that her account had been "hacked." While admitting that the witness' explanation was tenuous at best, the Appellate Court of Connecticut found that the Facebook printout was indefensible and thus inadmissible.

Looking at Facebook alone, there are three different options available to attempt to capture information on the social media site. The first option is image cap-

ture, by either taking a screenshot or printing a page of a user's profile. However, this method will not capture metadata, and, as evidenced by the *Griffin v. State* ruling, is not necessarily defensible. Since this type of image capture could very easily be generated or edited by anyone, this type of capture may not be admissible in court.

The second option for collecting data is Facebook's built-in download tool. Using this tool, it is possible to download all information from the user's timeline (contact information, interests, groups, etc.), content that the user or his/her friends have posted on his/her timeline, photos and videos that the user has uploaded to their own account, the user's friend list, notes the user has created, events to which they have RSVP'd, messages that they have sent or received, and comments that the user and his/her friends have made on the user's timeline content. Although this seems much more inclusive in terms of data collection, this method of gathering information is not flexible. By collecting social media information in this manner you are required to download all of the aforementioned content since the account's inception, creating a tedious amount of information to sort through. Using this method, one cannot set parameters for downloading content or search terms in order to pinpoint certain posts or timeframes, resulting in an excessive amount of superfluous data. Furthermore, no metadata is captured, so, even though it is more thorough than the first option, the same defensibility issue still stands. Even more problematic with this option is that the individual's username and password are required to utilize this tool—so it is useless without the cooperation of the witnesses and parties you are searching.

The third option of data collection involves specialized software that takes the next step beyond static data capture. With this software, we can collect the full range of authenticated metadata. Thus, the defensibility of the metadata is maintained by accessing the social media sites in a read-only mode, ensuring that none of the data is altered upon compilation. To ensure the integrity of the data, we calculate a MD5 hash value, which acts as a unique and secure identifier which is maintained through to data export. Video content can also be captured securely through the inclusion of the metadata encrypted with the video. Through this method, the social media information is preserved in a searchable, native format. The result is a defensible and searchable document, which allows for filtering out information and time frames unrelated to your case, saving time and effort. This method can also be used to verify or refute image capture evidence used by the opposing counsel at trial.

This software can perform either public or private data collection. Based on your cases' needs, the public information from a user's social media site(s) can be collected, or, with a username and password provided, everything the user has posted can be collected.

This major change in technology has opened new doors for e-discovery. It allows law firms and corporations to target information from social media sites in ways that is defensible, and provides greater ease to access. Now that there has been an explosion in cases citing Facebook, Twitter, and other social media outlets, there is an extreme advantage in capturing this information in a thoroughly defensible manner to make sure the information carries all of the necessary credibility with the courts. The emergence of this technology also provides the basis to question the manner of collection and defensibly of evidence that is produced by your opposition. Now you not only have all of the information you need, but you can rest assured you will be able to use it at trial.