The Social Media Gold Mine, a Wealth of Information for the Criminal Defense Lawyer.

Philip H. Hilder¹
Paul L. Creech²
Hilder & Associates, P.C.,
Houston, Texas

Whether it is Facebook, Twitter, or Google+, social media networks are now used by half of all Americans. They connect to them iPad, smart phones, and computers, while at work, watching television, and even while driving. There are those who even connect before, during, and after committing criminal acts.

With social networking becoming mainstream, the ability to understand and utilize these networks may make the difference between a favorable or unfavorable outcome in defending a client. One criminal defense attorney used a Facebook status update made by his client as an alibi that convinced a New York City District Attorney to drop an aggravated robbery charge. Knowing about, understanding, and being able to use social networking allows a criminal defense attorney to acquire the most valuable of all resources: information. Whether performing preliminary background research on a new case or unpicking a jury, social networks offer a wealth of information. In fact, Forbes.com recently instructed clients to start looking for a new attorney if they discover their lawyer does not have an iPad, a sign they lack the ability to understand and use technology in their criminal defense.

Using Social Media to Defend a Criminal Case.

In a criminal case, discovery can range from minimal to daunting. A trip though social media can provide insight into parties, expose relationships, and may provide that crucial evidence that exonerates. In recent years we have become accustomed to feeding Google with the names of witnesses, defendants, victims, and even law enforcement officials when investigating a case. Now we must add Facebook, Twitter, and growing number of 'check-in' sites to our investigation. Facebook profiles can be protected with privacy settings, many are not, and clients can give access to their accounts for the purpose of an investigation. A user's profile contains as much information about a person as you can possibly need: age, email address, phone number, religion, friends, where they work, their interests, and sometimes their every waking thought and feeling.

Information on social networks.

The real gold may be found in two places: status updates and photos. Users update their status to tell their friends what they are doing. A 19 year-old posted an inside joke to his Facebook about hanging out with his pregnant girlfriend and how his family went to IHOP without him, and it was that status that provided him with an alibi when he was arrested and charged with first degree robbery. Users have conversations with each other by way of posting on each other's Facebook walls, and often without regard to who can view their messages or download the photos. Users can 'tag' each other in

pictures so that a user can see all the pictures of a person 'tagged' no matter who uploaded the photo. Often people upload their whole photo library, regardless of how unflattering the photos may be, or whether they show illegal conduct and 'tag' their friends in each photo. The whole host of a person's social interactions can be documented in photos and memorialized in status updates, messages, and chats ready for your investigation. Social networks can help create a timeline, help you understand the interactions of persons involved, and provide exculpatory evidence.

Another kind of emerging social media are the 'check-in' websites, like Foursquare, which update other users as to the exact physical location of other users (Facebook has incorporated a similar feature). When a person goes to a new location (usually a business) they check-in using their mobile device. The status usually identifies the time, date, location, other users present, and sometimes a short message. Sometimes they do this to get coupons, but generally the purpose to alert other users of where they are and what they are doing. Users going places together will often 'check-in' together in a linked status.

Impeachment and Changing the Narrative.

Social networking websites are a gold mine for another invaluable pool of information: impeachment evidence. Because the essence of social networking is the communication of daily events through short timely text messages, photos, and public communication between people, it is very likely that witnesses have had posted status updates relating to their testimony at the time of the event and leading to trial. Witnesses' connections, statuses, friends, statements, photos, and other posted information may provide evidence of bias and prejudice for or against parties, minority groups, laws, or expose the complaining witness as not credible.

A witness may voluntarily have posted information that calls their ability to testify about any matter truthfully into question. They may have posted information about their own illegal activities, and possibility even photos. Social networks allow people to make short statements all day and night, some of which my contradict testimony they give. Nowhere else do you have access to hundreds, maybe thousands, of impulsive statements, often created in the heat of the moment and posted to the internet instantly using mobile devices.

The uncensored stream of consciousness postings by a person, combined with exposed relationships, and photos can be useful in changing the narrative of a case. Sometimes it is possible to use the information found on social media to enlighten the prosecutor to the full narrative and cause the prosecutor to lose interest in pursuing charges against a client. This alternative narrative maybe shed light on a complaining witness' activities for which they may have criminal exposure and may realign the focus away from a client. When the complaining witness' credibility is severely called in to question by their own postings, photos, and relationships reveled by social media, a criminal case may simply fall apart.

Undercover law enforcement on social networking.

It is becoming increasingly likely that an entire criminal case is based on social networking. Police, federal agencies, and school administrations have used false personal profiles to 'friend' targets and monitor hundreds of persons to collect information about illegal activities. When a person receives a 'friend request' from an undercover law enforcement official the request will come from a person with a complete profile to include pictures, favorite music, daily status updates, and the person will likely already have mutual friends to make the target feel comfortable with the user. One tactic is posing as a high school or college age female and request friendships with males to infiltrate a group of friends and monitor them for criminal behavior. Once 'friended' undercover law enforcement officers may be automatically granted access to hundreds of photos and years of daily status updates and wall-to-wall communications. Users who boast about illegal activities, giving times, dates, persons involved, and even photographic, audio and video evidence of criminal conduct with their 'private friends' are actually communicating it directly to law enforcement.

The undercover law enforcement activities may never be disclosed, and continue during and after trial. Evidence that is used at trial may appear to be wholy independent of the social networks. In this type of case the law enforcement uses social networks to discover when and where other evidence of a crime may exist or when and where a criminal activity is likely to take place. Law enforcement then develops probable cause on that secondary basis, without disclosing their ongoing social media monitoring.

Social media websites may be working complicity with law enforcement. While a social network may require a subpoena to reveal to law enforcement the user identified "private" data, they are susceptible to turning over data with just a request. Terms and conditions that govern user data provide outs for companies who wish to comply law enforcement requests. Social media companies are weary of appearing to be an unsafe place for teens, and have been cooperative with law enforcement requests for access and information. Social media websites also store data, most for at least a year, even after users have 'deleted' the data, for the purpose of retrieval by law enforcement.

Cyber-crimes.

The proliferation of internet based criminal activity, such as cyber-bulling, the posting of gang related material, and the making of threats requires criminal defense attorneys to understand how these websites work because you cannot rely on the representations of the prosecution that a specialized internet crime has been violated. Unless you understand how these social networks work you may be at a disadvantage to defend the activities of a clients on these websites.

Incriminating evidence.

While sometimes clients can be exonerated due to their attorneys understanding social media, Facebook updates can also backfire on a client. A 16 year-old boy who was convicted of murdering a 15 year-old girl, tried to create an alibi for himself by posting status updates on Facebook that stated he was watching television. He was so bold as to cryptically post status updates that referenced the payoff

of bet with a Facebook friend, the bet was that the friend would owe him breakfast if the suspect killed the young girl. The suspect also posted that he felt sorry for the girl's mother after the girl was reported missing. His Facebook posts were used against him at his trial to paint him as a devious, calculating, remorseless murder. 9

Using Social Media in Jury Selection.

Another area that attorneys have discovered a use for social media is in jury selection. Not searching for information about each potential juror on Facebook and with Google is a severe information disadvantage. In Cameron County, Texas the District Attorney's Office announced they would be using juror Facebook profiles and postings when selecting juries. In today's high tech, wi-fi enabled, iPad friendly courtrooms looking up a prospective juror's Facebook profile potentially reveals a host of bias, thought processes, and other information that can be used in voir dire.

The currency of exploring another's social media is information. Any information may give an indication of where a person's sympathy lies, how opinionated they are, or whether they are erratic. A person who is a fan of one or all of the CSI permutations may have unrealistic expectation of the amount, type, and quality of scientific and forensic evidence than another person. Criminal defense attorneys who would turn the CIS effect to their advantage would be more advantaged having a self-proclaimed fan of the show on their jury. If defending a minority for a crime it would be nice to know if the jurors have close minority friends that they interact with on social media. But, more than that social media has become a place of political expression, to can learn if someone is liberal, conservative, anti-corporate, has environmental concerns, and how opinioned they can be.

Social media will aid you selecting a jury, in choosing a theme for the case, and in presenting the theory of the case and who the jurors are as people, what they care about, and how they think. In a case where a black man was charged with sexual assault, a defense attorney kept a white woman on a jury after discovering pictures of her with black male friends on Facebook. ¹¹ In a products liability case, a juror was struck after the defense team discovered the juror posted unsolicited advice and strident opinions on Facebook. ¹² In another products liability case a juror was struck after she posted that Erin Brockovich was her hero. ¹³ A student who hosted an anti-corporate blog was struck from another products liability case. ¹⁴ You may be able to learn very quickly what kinds of books potential jurors read, movies they watch, televisions shows they watch, their thoughts on the day's trial of the century, there thoughts on current events, and then use this information to help you unpick a jury.

One issue that may give pause is that people may be constructing their online image based on who they want to be rather than on who they are.¹⁵ Their true sympathies may be different than there published feelings. A person may wish their friends to perceive them in a certain way, as a cool or interesting person. They may be parroting another's views on issues of style, culture, or politics and in the jury box they may follow a crowd or their true impulses may be revealed. Still, any information to prepare or supplement voir dire questioning gives an advantage and aids the process.

The amount and type of information not protected by privacy tools may reveal as much as what is revealed. A person with a public profile who posts continuously will likely have shared that they have

been selected for jury duty and expressed some opinion on it. The users of social media are likely to reveal at least some information about themselves not readily available another way.

Conclusion.

Be wary of ethical pitfalls. Creating a phony Facebook or other profile to trick a person to 'Friend' you so that you can snoop in their private Facebook account is likely a violation of the Model Rules. You can subpoen the same information without being dishonest or requesting your employees or anyone else to act dishonestly.

Social media is here to stay. According to recent studies, the users of social media are prevalent among the rich and poor, old and young, all races, all education backgrounds, and are used in the city, the suburbs, and on the farm. ¹⁶ If you are not searching social media in part of preparing a defense for a client or jury selection, know that your adversary will be using these tools. Mastering social media searches may give a short term advantage, but soon, not using it will be a great disadvantage as the profession adapts to another new tool in the arsenal.

¹ Phillip H. Hilder is a former federal prosecutor and founder of Hilder & Associates, P.C., located in Houston, Texas. Mr. Hilder focuses on white-collar criminal defense matters. He is co-founder of the ABA National Institute on Securities Fraud. He had been the Attorney-in-Charge of the Organized Crime Strike Force, Houston Field Office, and was an assistant U.S. Attorney for the Southern District of Texas. Hilder & Associates , P.C., 819 Lovett Blvd., Houston, TX 77006-3905; (713) 655-9111; www.hilderlaw.com.

² Paul L. Creech is a graduate of the South Texas College of Law, cum laude, Order of Lytae, Phi Delta Phi, where he was a member of the South Texas Law Review. Mr. Creech is former U.S. Marine.

³ Half of adults in U.S. are users of social networks, study says, Houston Chron., August 26, 2011, at B8.

⁴ Vanessa Juarez, *Facebook status update provides alibi*, CNN.com, November 12, 2009.

⁵ Kashmir Hill, *Make Sure Your Lawyer Knows How to Use Facebook*, Forbes.com, February 2, 2011.

⁶ Vanessa Juarez, Facebook status update provides alibi, CNN.com, November 12, 2009.

⁷ Lisa Dowd, *Teenager Killed Girl After Free Meal Offer*, Sky News.com, September 2, 2011.

⁸ Claire Ellicott, *The schoolgirl killed for a bet: Boy, 16, was dared by Facebook friends to murder in exchange for a free breakfast,* DailyMail.co.uk, July 28, 2011.

⁹ Vanessa Juarez, *Facebook status update provides alibi*, CNN.com, November 12, 2009.

¹⁰ Laura B. Martinez, *Cameron Co. DA will check Facebook profiles for jury picks,* Brownsville Herald, January 17, 2011.

¹¹ Kashmir Hill, *Make Sure Your Lawyer Knows How to Use Facebook*, Forbes.com, February 2, 2011.

¹² *Id*.

¹³ Id.

¹⁴ *Id*.

 $^{^{15}}$ Ana Campoy and Ashby Jones, Searching for Details Online, Lawyers Facebook the Jury, Wall Street Journal (WSJ.com), February 22, 2011.

¹⁶ Half of adults in U.S. are users of social networks, study says, Houston Chron., August 26, 2011, at B8