37-SPG Fam. Advoc. 32

Family Advocate
Spring, 2015

Feature

SOCIAL MEDIA AS EVIDENCE: NAVIGATING THE LIMITS OF PRIVACY

Simon R. Goodfellow [a1]

Much has been written in the last few years about the rules governing the growing use of social media evidence in litigation. After all, social media is a relatively new phenomenon. Facebook was founded in 2004 and, in just ten years, has 1.3 billion monthly active users. If Facebook were a country, it would soon be--or might already be--the most populous country on the planet.

When you look at the rules for social media evidence, you quickly realize that the rules are not new. Only the context is new. Indeed, in 2010, a U.S. District Court in Indiana noted that using social media evidence simply "requires the application of basic discovery principles in a novel context." Thus, rather than needing to learn new rules to keep up with ever-changing technology, once we realize the parallels that can be drawn between the real world and the online world, the rules we already know should work just fine.

Parallel worlds

Imagine a plaintiff in a personal-injury action who claims he hurt his back. The defense attorney suspects that he is not as badly injured as he claims. Long ago, before the Internet and social media, one of the tricks a defense attorney's private investigator might use (or so I hear) was to scatter cash over the claimant's front lawn, knock on the door, hide, and then videotape the claimant running around and bending down to pick up the money. But what if the plaintiff claims the video violates his right to privacy because he was in his own front yard? The answer is he likely would be out of luck.

We all have a constitutional right to privacy. For example, the Fourth Amendment to the United States Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures ...."

Likewise, the California Constitution provides:

> ***33** All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and *privacy*.

In California, the right to privacy includes "precluding the dissemination or misuse of sensitive and confidential information." To prove a violation of this right to "informational privacy," a plaintiff must prove: (1)

a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) a serious invasion of the privacy interest.

In the physical world, the law holds that there is no reasonable expectation of privacy as to events: (a) in plain view; (b) from a public place; (c) where the observer has a right to be. Thus, in the example above, if the plaintiff's conduct was visible from a public place--for example, if the investigator videotaped the plaintiff from behind a tree on the public parkway in front of the plaintiff's house--the plaintiff could not argue that he had a reasonable expectation of privacy as he ran around picking up cash on his front lawn.

Nowadays, from the comfort of her desk, an attorney handling a personal injury, divorce, or other kind of case can with a few mouse clicks find all kinds of information about the opposing party or witnesses. But are there privacy limits to the use of online evidence?

Expectation of privacy

When answering this question, it helps to think of the plaintiff and the investigator described above. Whether the plaintiff was picking up money on his front lawn or doing Zumba in his living room with the drapes open, the key question is the expectation of privacy and whether the conduct was in plain view from a public place where the observing investigator had a right to be.

As an example, a California court denied an invasion-of-privacy claim by a judge who while leaving his home was filmed by a camera crew parked across the street. The court reasoned that the judge was in public view and the news crew did not enter his home, physically contact him, endanger his safety or that of his family, or disclose where he lived.

In 2013, a judge in New York dismissed a lawsuit against a photographer who had exhibited in a gallery photos he had taken through his neighbors' windows using a telephoto lens. In contrast, a California court held that a woman's privacy had been invaded when a film crew riding along with paramedics entered her home without permission, filmed the paramedics failing to resuscitate her husband, and then aired the footage on TV, also without permission.

The same law and logic extend to the Internet, such that if the attorney is on a webpage that is publicly available without having to, for example, hack it or steal the password, privacy rights do not bar use of the evidence in litigation. In the last few years, the Sixth Circuit, the Maryland Supreme Court, a Minnesota court of appeal, and an Ohio court of appeal, among others, have all ruled that information posted online, with no restrictions as to who could see it, is public information for which the poster could claim no reasonable expectation of privacy.

Indeed, recent cases abound in which publicly available online information was used against a party or a witness in litigation. For example, in a 2010 New York case, a plaintiff claimed that injuries confined her to bed, but the court admitted evidence from the plaintiff's Facebook and MySpace pages showing her leading an active life. Similarly, in a 2007 Ohio case, the appellate court affirmed a lower court's award of child custody to the father, when the mother's MySpace page included her statements that she practiced sadomasochism and used illegal drugs.

Thus, just as the private investigator mentioned above could videotape the plaintiff because he was in plain view from a public parkway, a family law attorney may search the Internet for publicly available information and photos concerning the opposing party.However, just as the investigator could not have broken into the claimant's house and stolen his diary--without violating the plaintiff's reasonable expectation of privacy--the attorney may not use hacking, stolen passwords, or other covert means to access the opposing party's online information. For example, both the Philadelphia and New York Bar associations have stated that a lawyer may not ethically have a third party send a "friend" request to a witness on Facebook, without revealing the affiliation, in order to access incriminating or otherwise useful information.

*34 To prevent the investigator from accessing damaging evidence in his home, the plaintiff in the example above simply had to close his door and drapes so that the investigator could not see inside from a public place. Similarly, to prevent an attorney from being able to use online evidence against him, the plaintiff simply could adjust his online privacy controls to block public access. For example, when posting on Facebook, one can choose who can see one's posts--the whole world, just "friends," just family, or solely people one specifically chooses. However, many social media users are not knowledgeable about what is public and what isn't.

In 2012, *Consumer Reports* estimated that 13 million U.S. Facebook users chose not to change--or were not even aware of--their Facebook default privacy settings. Of Facebook's 1.3 billion monthly active users, about 864 million log on daily. Every minute, they "post" 246,000 times, and they "like" something 1.8 million times. Twitter has 284 million monthly active users who send 500 million tweets every day. YouTube users watch more than six billion hours of video every month, and they upload 100 hours of video every minute.

Until restricting access to information online becomes as easy as closing your front door and drapes, lawyers will continue to have access to a treasure trove of information through which they may search for a case's smoking gun or silver bullet. Indeed, a survey in 2010 by the American Academy of Matrimonial Lawyers found that 81 percent of its responding members reported searching for and using social media evidence.

The partially opened door

But what if the opposing party *has* limited access to his or her social media information? Again, think of the plaintiff described above. Obviously, just because certain evidence is inside the plaintiff's house does not mean that the defense attorney cannot obtain it. The attorney simply must use formal discovery. During the plaintiff's deposition, defense counsel can ask questions about the plaintiff's physical activities, hobbies, etc. She can propound requests for all documents concerning the plaintiff's injuries. Assuming the documents can lead to admissible evidence, the plaintiff cannot object to producing existing, relevant documents purely on privacy grounds because the documents are inside his home. Similarly, a party who has used social media, but has privacy-protected the information from public view, cannot refuse to give up posted information on the grounds of privacy.

For example, in the 2010 New York case mentioned above, the court granted a motion to compel access to the private portions of the plaintiff's Facebook and MySpace pages. The court held that since the public portions included images of her smiling happily outside her home, despite her claim that injuries confined her to bed, there was a reasonable likelihood that the private portions of her social media pages would contain

similar information that would be "both material and necessary to the defense of th[e] action and/or could lead to admissible evidence." The court further held that the defendant's "need for access to the information outweigh[ed] any privacy concerns that may be voiced by [the plaintiff]."

The attorney whose investigator obtained the video of the plaintiff picking up cash on his front lawn would still have to deal with issues such as authentication in order to render the information admissible as evidence at trial. The same goes for social media evidence. The fact that it came from the Internet does not alter the requirements of authentication and relevance. For example, in a 2009 Missouri criminal case involving charges of rape, the court excluded evidence of the victim's Facebook entries concerning prior drinking, partying, dancing, sexual relations, and memory loss as irrelevant to the events on the night in question.

Authentication might include (1) testimony from the person who printed the webpage that it is a true and correct copy, and (2) direct or circumstantial evidence that the party or witness it is being used against posted the statement on the webpage.

Thus, the attorney who safely navigates the uncharted waters of social media evidence is the attorney who does not get distracted by the new context, but simply understands the parallels between the physical world and the online world. In both worlds, the rules of discovery and evidence still apply.

Footnotes

a1 **SIMON R. GOODFELLOW** is an associate in the business litigation group of Bartko Zankel Bunzel & Miller in San Francisco.