

How to Gather Social Media Evidence

Table of Contents

1. Introduction	3
2. Accessing Social Media in an Investigation	4
3. Tools and Techniques for Gathering and Preserving Social Media Evidence	5
4. Authenticating Social Media Evidence	5
5. Case Examples and Court Decisions	6
- Zimmerman v. Weiss Markets	7
- The Rodney Bradford Case	7
- Arcq v. Fields	7
- Griffin v. State of Maryland	7

Introduction

Social media evidence can be a valuable addition to an investigation, revealing the kind of information that, years ago, would have been difficult, if not impossible, to find. But it has to be gathered in a way that will hold up in court. Because it's such a new source of evidence in investigations, case law is developing rapidly. A forward-thinking investigator would be well-advised to stay on top of the latest rulings.



Accessing Social Media in an Investigation

With so much information being exchanged and shared online, it makes sense to see social media as a rich source of material for both plaintiffs and defendants to use in investigations, but getting access to the relevant data isn't always a simple matter of clicking on a page. Many users of social media have privacy settings that restrict access to the information they post.

In certain cases, the court has ordered that passwords be disclosed, but this is extreme. The decision to order the exchange of log-in information has been based on evidence showing that something relevant to the investigation is probably in the private or non-public part of a social media page.

A judge might request a user to provide the evidence from his or her own social media pages to lawyers for the other side. But without a formal request for disclosure, investigators and attorneys may be left with some difficult dilemmas.

Recent cases in which parties in a dispute have 'friended' someone to gain access to their social media posts have shed light on what the courts consider to be acceptable. Evidence gained by this kind of deception has not held up so far. It also violates the terms of service set out by some social media platforms and has prompted some states to address the practice in writing.

The California Penal Code 528.5 says: "Any person who knowingly and without consent credibly impersonates another actual person through or on an Internet Web site or by other electronic means for purposes of harming, intimidating, threatening, or defrauding another person is guilty of a public offense."

The Connecticut Rules of Evidence Section 52-184a says: "No evidence obtained illegally by the use of any electronic device is admissible in any court of this state."

Even when information is publicly available, though, there can be legal issues related to its discovery, warns attorney Benjamin Wright, who is an expert in e-discovery as well as an author and instructor at SANS Institute. These can include copyright violations and privacy violations based on statements they may have written on their social media pages.

The amount of data an investigator seeks permission to collect should be proportionate to the case under investigation. Wright says that "if the request is not targeted, proportionate to the seriousness of the case and rationally based on already-known evidence, the request may be blocked." Investigators need to have a sense of restraint and have a good reason for requesting the information.

As Pennsylvania employment lawyer Eric Meyer writes in his blog post, [Your employees' "private" Facebook posts are not private](#), "the party seeking discovery of evidence must be able to demonstrate that the information sought is reasonably likely to lead to the discovery of admissible evidence." This means that employers can't go rooting through an employee's social media accounts in hopes of finding

No evidence obtained illegally by the use of any electronic device is admissible in any court of this state.

- Connecticut Rules of Evidence

something. Requests to access an employee's social media account(s) must demonstrate a valid reason to believe that there's information in their profile that's relevant to the issue under investigation.

Tools and Techniques for Gathering and Preserving Social Media Evidence

Once the access to social media information has been secured, either through court order or simply due to public accessibility, evidence must be gathered in a way that is legal and useful. Collecting [evidence from social media sites](#) can be challenging for several reasons. Social media is constantly changing, and users can easily update and delete material that could be evidence in a case, although once a user is aware of an ongoing investigation, he or she is under an obligation to preserve social media evidence just as if it were any other type of evidence. Deleting photos, posts and other information is akin to shredding documents and the courts have been clear about the consequences, handing out hefty fines and sanctions for spoliation, as a Virginia lawyer and his client found out in a recent [wrongful death case](#).

So far there are relatively few standardized, widely accepted methods for gathering evidence from social media sites, says Wright. "A common approach is for someone to just try to print what they see on their screen onto a piece of paper and show it to the judge or administrator," he says. However, printouts don't always contain all of the information and the interactivity that takes place on social media sites. A better alternative to the printout is a screencast.

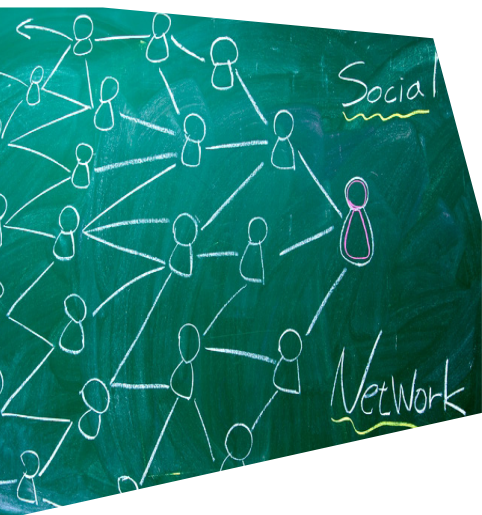
A screencast captures the look, words, images, interactivity and inter-relationships from one page to the next. It's a valuable tool because what's on a social media profile today may not be there tomorrow. Wright suggests using a webcast narration, where the investigator records a video of him/herself talking about what they are seeing on the page. There are several effective tools for this, including Camtasia and Screencast-O-Matic.

If what you're looking for is on Facebook, Meyer suggests using Facebook's "[Download Your Information](#)" function, which allows a user to create an electronic copy of his or her entire profile. This includes contact information, interests, groups, wall posts, photos and videos, friend list, notes, events, private messages, comments, and other related content.

Authenticating Social Media Evidence

But accessing and gathering the information in a format that you can present as evidence is only half the battle. You still need to prove that it's authentic, given the possibility of impersonation and digital fabrication in the online world.

Since information on social media profiles is not immediately verifiable, printouts are not generally admitted as evidence on their own. The Federal Rules of Evidence dictate that material taken from social media accounts generally requires additional corroboration to link the printouts to the account holder in order to consider the information as evidence.



To authenticate a screencast, Wright recommends that you create a script of what you are going to say in the screencast as you capture evidence.

The script should include:

- Investigator's identity – who you are, purpose of the screencast
- Date and time of the screencast
- A statement that acts as your signature, authenticating what you see and the statements you have made

Wright also recommends that you then corroborate the date and time of the recording by:

- Emailing the video to several people, including yourself, your boss and the attorney who is advising the investigation.
- Uploading the video to a secure enterprise resource or third party service that shows an audit trail of time and activity. The i-Sight case management system for investigations contains a mechanism for uploading video files in any format, attaching them to the case file with a date and time stamp.

The court ordered Zimmerman to hand over his passwords and login information to the counsel for Weis Markets so that they could access the private sections of his Facebook and MySpace accounts.

Case Examples and Court Decisions

Request for user names and passwords granted: Zimmerman v. Weiss Markets

In the *Zimmerman v. Weis Markets Inc.* case, Zimmerman was an employee of a subcontractor of Weis Markets and was seeking damages for an injury that occurred at work. Zimmerman claimed that an accident seriously and permanently impaired his health. Weis Markets reviewed the public portions of Zimmerman's Facebook and MySpace pages, and felt that there might be some additional information to refute the damage claims in the private sections of his profile.

On the public portions of his profile, the company found photos of Zimmerman engaging in some of his favorite activities after the accident took place at work. They knew the photos were from after the accident because his scar from the accident was visible in the pictures.

The court ordered Zimmerman to hand over his passwords and login information to the counsel for Weis Markets so that they could access the private sections of his Facebook and MySpace accounts. The opinion released by the court said:

"Zimmerman voluntarily posted all of the pictures and information on his Facebook and MySpace sites to share with other users of these social network

sites, and he cannot now claim he possesses any reasonable expectation of privacy to prevent Weis Markets from access to such information.

“By definition, a social networking site is the interactive sharing of your personal life with others; the recipients are not limited in what they do with such knowledge. With the initiation of litigation to seek a monetary award based upon limitations or harm to one’s person, any relevant, non-privileged information about one’s life that is shared with others and can be gleaned by defendants from the internet is fair game in today’s society.”

Facebook status update used to corroborate an alibi: The Rodney Bradford case

In another case, a New York teenager’s Facebook status update provided evidence that helped to keep him out of jail. The teen had been arrested for a mugging in Brooklyn. Despite his insistence that he wasn’t connected to the crime, the boy spent nearly two weeks in jail before his father discovered a Facebook status update he had made from his Harlem apartment one minute before the mugging, which was 12 miles away.

The boy’s father presented the Facebook evidence to the district attorney, who then went on to submit a subpoena to Facebook to verify the location from which the status update was made. The time stamp and the location were used as evidence to prove that the boy wasn’t at the scene of the crime. He was cleared of the charges based on the electronic evidence.

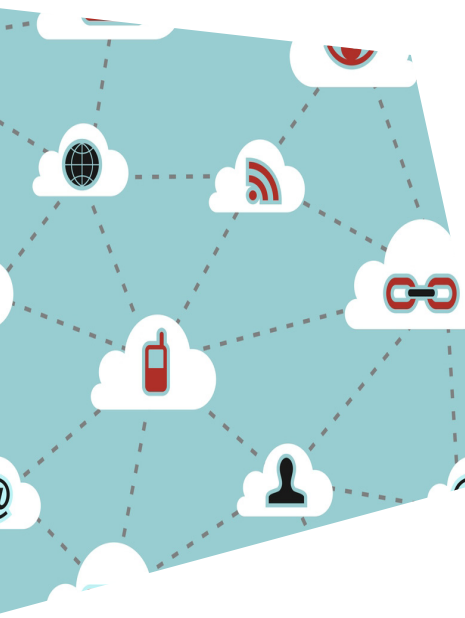
User name and password request denied: Arcq v. Fields

In this case, James Arcq was seeking damages because of an auto collision, claiming that the driver of the other vehicle, Robert Fields, was negligent. Arcq claimed that the accident resulted in an inability to participate in certain activities. The defendants in the case believed that Arcq had profiles on social media sites, and requested that user names and passwords to all of Arcq’s profiles be handed over. The defendant’s request was not made based on information obtained by viewing the public contents of Arcq’s social media profiles.

In the [opinion document](#) in the Arcq v. Fields case, the request to hand over social media username and passwords was denied because the defendant wasn’t able to show a valid reason to believe that there was relevant information on the plaintiff’s social media profiles. The opinion also mentioned that the defendants in the case didn’t seem sure that Arcq even had any social media accounts.

Evidence not properly authenticated: Griffin v. State of Maryland

In the [Griffin v. State of Maryland](#) case, Griffin had been charged with multiple counts in the death of a man at a bar. Prior to the trial, Griffin’s girlfriend allegedly threatened one of the witnesses on MySpace. The witness that was



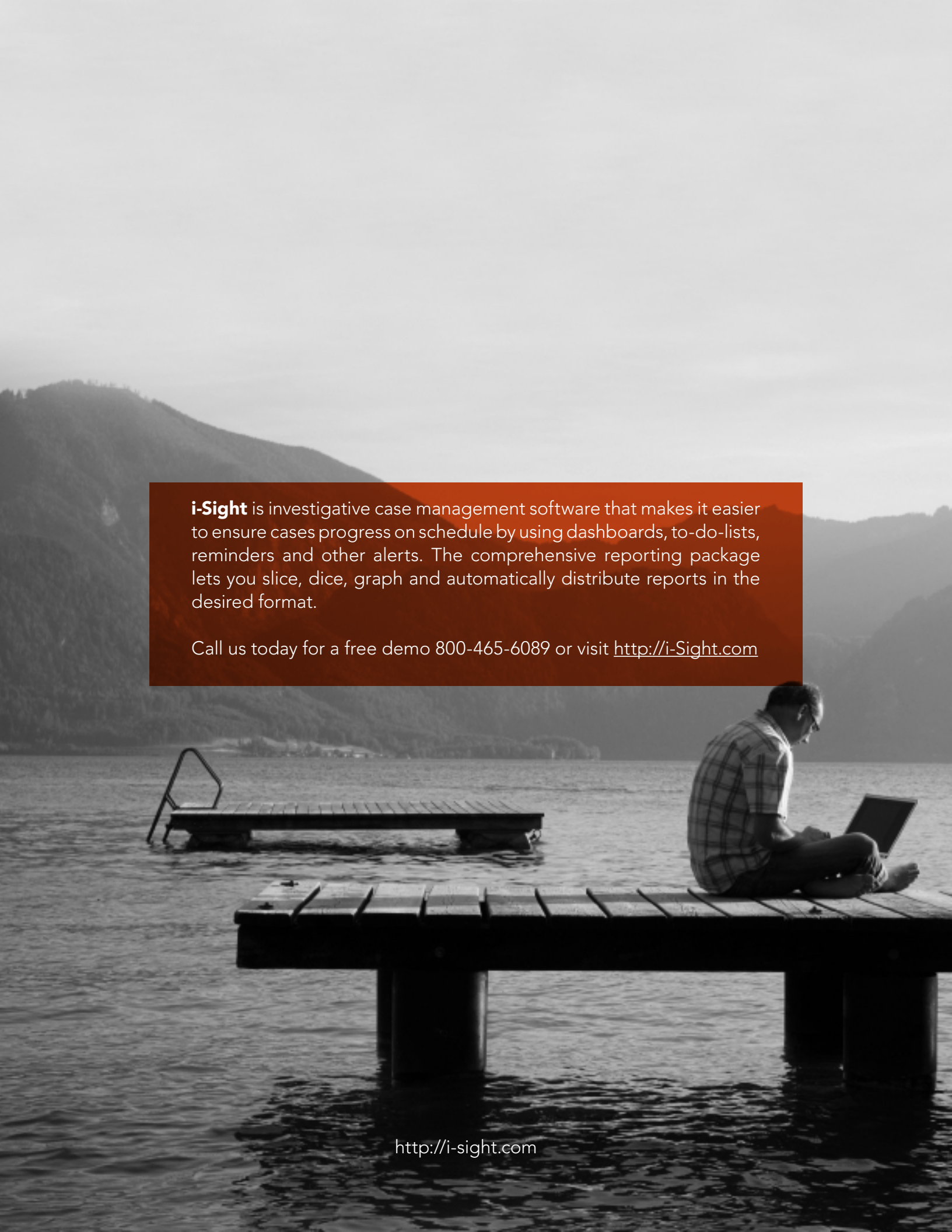
allegedly threatened gave two different versions of his story in the first and second trials, later explaining that there was a discrepancy in his stories because he was threatened prior to the first trial.

On the day after Griffin's girlfriend testified, the State introduced pages that had been printed from a MySpace account. The account was in the name of "SISTASOULJAH" and had the same birthday and hometown as Griffin's girlfriend. There was also a photo of a couple on the page, which counsel and the court agreed appeared to be a picture of Griffin and his girlfriend.

Defense objected to the use of the MySpace printouts in the case because Griffin's girlfriend was never questioned about the MySpace account and whether or not it belonged to her. It could not be determined exactly when the message containing the threat was sent, and it also couldn't be verified that Griffin's girlfriend was the one who sent the message. It was argued that anyone could have set up that page and posted the threat.

The Maryland Court of Appeals reversed and remanded for a new trial the defendant's murder conviction for the State's failure to properly authenticate the MySpace pages. The court found the trial judge abused his discretion in attempting to authenticate the MySpace post through the lead investigator's testimony only. The court found that the picture of the girlfriend, coupled with her birth date and location, were not sufficient to authenticate the printout.

Defense objected to the use of the MySpace printouts in the case because Griffin's girlfriend was never questioned about the MySpace account and whether or not it belonged to her.



i-Sight is investigative case management software that makes it easier to ensure cases progress on schedule by using dashboards, to-do-lists, reminders and other alerts. The comprehensive reporting package lets you slice, dice, graph and automatically distribute reports in the desired format.

Call us today for a free demo 800-465-6089 or visit <http://i-Sight.com>

<http://i-sight.com>