Using Social Media in Investigations

Case IQ™

While social media can offer a wealth of information for investigators, one wrong move can render a key piece of evidence unusable. So how can investigators mine this incredibly rich resource without getting into hot water? Navigating the sometimes murky world of social media takes an understanding of three key concepts: access, preservation and authentication.

This guide explains how investigators can safely manage all three processes to ensure valuable evidence stands up to scrutiny.

Preservation

Since social media is constantly changing, evidence viewed on one day can disappear the next. It's important for any evidence to be captured and preserved as soon as it is found. This can be done several ways.

Screencasts can be used to capture words, images and the interactivity between pages. Using a webcast narration allows investigators to record themselves talking about what they are seeing.

Facebook has a feature that allows users to download their entire history, creating an electronic copy of an entire profile. This can be useful when the activity in question occurred months or years earlier and a search is necessary to find the relevant information.

Sometimes subjects in investigations will willingly provide their Facebook histories. In other cases, an investigator may need to compel a subject to hand over the information.

Access

On some social media networks, such as Facebook, the bulk of personal information is stored on private profiles, posing an ethical dilemma for the investigator. Filing a formal delivery request to access the data through US courts, while possible, is not always an option for discrete investigations. It may be tempting to try not-so-ethical means to get access to private information. But posing as a "friend" to get access to a private page – known as pretexting – opens up the investigation to a long list of risks.

What is Pretexting?

Generally, pretexting is interpreted as using deceptive tactics or impersonation to gain access to information that would otherwise be unavailable to the public. It's usually deployed on social media in scenarios where a subject is unaware of, or unwilling to participate in, an investigation. An investigator, or his or her delegate, pretends to be an acquaintance or friend of the subject to get inside the person's network. It's a dangerous game that can result in valuable evidence being disregarded. But if an investigator openly adds the subject as a friend to gain access to their profile – without posing as an acquaintance – the move is usually considered in-bounds ethically.

Murky Legal Waters

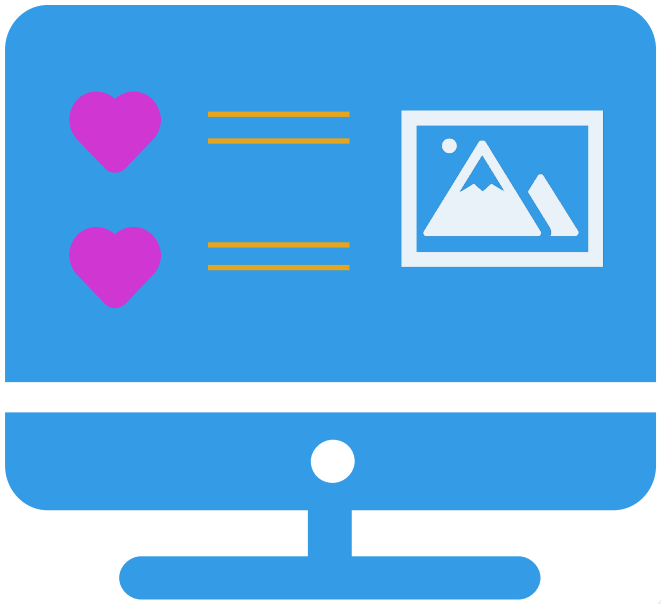
Bar associations across the country have panned pretexting as unethical for both lawyers and investigators. But evidence acquired through pretexting is occasionally deemed admissible – in US civil litigation, many courts have ruled that "the admissibility of evidence is not affected by the means through which it was obtained," the American Bar Association reports. The National Association of Insurance Commissioners drafted legislation that would allow insurance fraud investigators to use pretexting tactics when "there is a reasonable basis for suspecting criminal activity." The bill has been adopted by several states.

Know the Rules

Lawyers have been reprimanded and disbarred for presenting evidence from investigations that used pretexting techniques, and investigators can face major fines or even jail time in some states. In California, it's illegal to "knowingly and without consent credibly impersonat[e] another actual person through or on an Internet Web site."

Due to the ever-evolving nature of social media, laws surrounding online evidence gathering are often in flux as courts attempt to keep up. Legal precedent for pretexting varies from state to state and from industry to industry, since the financial sector is governed by different standards than say, the insurance sector.

Both the Gramm-Leach-Bliley Act and the Fair Debt Collection Act prohibit pretexting as a means to obtain personal financial information or "attempt to collect any debt." But even when guidelines are unclear, investigators are encouraged to avoid pretexting, since it is widely recognized as unethical.



Authentication

Regardless of how they find evidence online, investigators are required to ensure content from social media is authentic. Verifying the content can be as simple as asking the subject if they, in fact, posted the photo or message. But judges have, in the past, ruled evidence from Facebook inadmissible because an attorney suggested his client's account had been hacked.

Investigators are often forced to go as far as computer forensics work – for example, recording the IP addresses responsible for social media posts to verify who actually posted the content. Internet browsing history and witness testimony can also corroborate evidence.

Emailing les or videos to others or yourself can help to time-stamp the information. This is especially effective to corroborate the time that you made a screencast to preserve social media evidence.
An affidavit, signed by a witness, attesting to the investigator's findings on social media sites, can also be helpful proof of the authenticity of the evidence.

In a Nutshell

Social media networks are among the most valuable sources of online evidence, so keep these rules in mind to ensure you can use it:

1. Access the information ethically and legally
2. Preserve the information effectively
3. Authenticate the evidence to ensure its validity

Follow the rules to get the most out of this valuable resource .

www.caseiq.com/
1-800-465-6089
sales@caseiq.com

Case IQ™