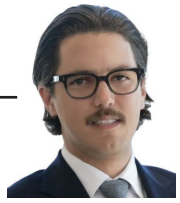
Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
July 2025

Joseph Younes
BD&J, PC



Garret Valerio
BD&J, PC

The digital minefield

EXPOSING AND DEFUSING SOCIAL-MEDIA SURVEILLANCE AT TRIAL

This article provides a practical playbook for identifying, obtaining, and neutralizing defense-led social-media investigation in California litigation.

A picture is worth a thousand words. Social-media content often shapes perception, but the meaning behind any post, regardless of its caption or context, is ultimately left to the viewer's interpretation. For plaintiffs, that interpretation is not always generous. In trial, it means a photo posted to social media of your client smiling at the beach can magically erase months of documented pain and suffering.

Many plaintiffs are unaware of the extent to which their online presence is accessible to their adversaries in litigation, or how easily their content can be misconstrued to their detriment. Posts, photos, videos, location check-ins, hashtags, comments, and even third-party tags can be selectively framed to undermine a plaintiff's credibility or to suggest injuries are exaggerated.

Digital surveillance: Understanding defense social-media investigations

As a relatively new form of "surveillance," defense-hired investigators now rely on advanced software and digital search tools to perform comprehensive analyses of a plaintiff's online presence. These investigations go far beyond a surface-level review of an individual's Facebook or Instagram page. They often include searches across more than 100 platforms, including obscure blogs, discussion forums, and app-based communities. In some cases, investigators can even collect content from individuals who appear to have no public online profile.

To minimize the effect of a defendant's social-media investigation into your client, it is important to understand the types of materials they are likely to receive from an investigative service after engaging them in a case. These typically include a detailed analyst report that preserves social-media content such as posts, photos, videos, and metadata, along with background checks, and open-source intelligence. Most materials are saved in formats that ensure authenticity through timestamps or encryption. Additional documents such as investigator notes, billing records, and service invoices are usually sent to the defense as well.

The first sign that defendants possess these materials often comes when they assert boilerplate objections based on attorney-client privilege or the attorney work product doctrine in response to discovery requests concerning social-media investigations. These objections frequently lack an accompanying privilege log or any factual basis for withholding the requested information. In response to such objections, it is essential to promptly meet and confer with defense counsel and demand a privilege log and an explanation for any claimed protections. This step is critical for identifying the full scope of social-media investigative materials in the defense's possession and laying the groundwork for a motion to compel if necessary.

Educating your client: Proactive guidance prevents future issues

It is essential to educate your client early in the litigation process about common defense surveillance tactics to prevent statements or actions from being taken out of context. After all, it's better to come from you than to come by surprise. Revisit these discussions ahead of key case milestones – such as your client's deposition, defense medical examinations, or while assisting with written discovery responses. Educate your client on what sub rosa is and how the defense will try to use it against them in a case. Explain to your client why the defense is entitled to carry out surveillance on them but also the ways in which you may limit their ability to utilize it in the case. Treat your client like a partner on this issue and explain why it is important that you work together to ensure they are careful with their social-media posts and online presence.

Remind them not to add any suspicious social-media account followers or friends on Facebook. Advise them to inform you if they suspect any suspicious activity on their social media platforms and let them know that surveillance is most likely to occur before or after their deposition and/or a defense medical examination. These are moments when the defense knows exactly where your client will be and at what time, which allows them to plan surveillance with precision and increase the likelihood of capturing content that can be taken out of context and later used to impeach your client.

Emphasize the importance of avoiding extreme or absolute language during depositions/discovery responses (e.g., "always" or "never"), as such terms can be used by the defense for impeachment purposes. This will assist you in setting up your argument in motions in limine. For example, if your client never said they couldn't walk and the defense has a video or photograph from social media of them walking, you can explain to the judge that the video is merely irrelevant since your client has never testified or said in discovery that

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
July 2025

he/she cannot walk or do the exact thing that the defense is trying to show them doing.

"To give evidence the label of 'impeachment,' does not always make it 'impeachment evidence.' In the law, we are more concerned with substance and merit, than we are with form and appearance." (*Newsome v. Penske Truck Leasing Corp.* (D. Md. 2006) 437 F.Supp 2d 431, 433.) Under California law, a witness's prior statement, to be properly subject to impeachment, must be "clearly inconsistent" with the evidence being proffered for impeachment purposes. (*Fibreboard Paper Products Corp. v. East Bay Union of Machinists* (1964) 227 Cal.App.2d 675, 699; see also, Cal. Evid. Code, § 780; 3 Witkin, Cal. Evid. (5th ed. 2012), § 351.) Unless the footage or post shows your client doing something they specifically said they cannot do, you may have a good chance of arguing that the material is not for impeachment, is irrelevant, and may mislead/confuse the jury.

Instruct your client to minimize social-media activity during the pendency of the case. One of the first few places that the defense will always check is your client's social-media account. As such, it should be one of the first things you do. Explain the importance of why your client should be very cautious about items they wish to post on social media as it can be taken out of context and used against them.

The law: Defense-led social-media investigations are discoverable

Despite what some defense attorneys argue, social-media investigations are not protected by attorney-client privilege or the attorney work-product doctrine.

California has long held that photographs, films, and audiotapes of surveillance are subject to discovery and, such evidence is not protected by the attorney-client or work-product privilege. (*Suezaki v. Superior Court* (1962) 58 Cal.2d 166.) Surveillance evidence does not constitute a confidential communication for purposes of the attorney-client privilege and further, that transmission of the evidence to the attorney, even where the parties intend the matter to be confidential, "cannot create the privilege if none, in fact, exists." (*Id*. at 175-177.)

In *Coito v. Superior Court* (2012) 54 Cal.4th 480, the California Supreme Court held that "the applicability of absolute protection must be determined case by case. An attorney resisting discovery of [evidence] based on absolute privilege must make a preliminary or foundational showing that disclosure would reveal his or her 'impressions, conclusions, opinions, or legal research or theories.'" (*Id.* at 495.)

Thus, with respect to witness statements from attorney-led interviews, a court may find absolute protection where the evidence would "provide a window into the attorney's theory of the case or the attorney's evaluation of what issues are most important." (*Ibid.*) Even when there is no window into an attorney's theories or evaluation, the evidence may still be subject to qualified work product protections to "prevent an attorney from free riding on the industry and efforts of opposing counsel." (*Id.* at 496.)

Defendants face significant difficulty in meeting this burden when it comes to withholding social-media investigation materials from discovery. Materials such as digital-surveillance reports, metadata logs, screenshots, and online activity summaries typically originate from independent third-party investigators and often consist of factual, publicly accessible information. These materials are not prepared by attorneys, nor do they reflect legal strategy, mental impressions, or case theories. They are gathered through standardized investigative methods and do not contain attorney analysis. Hence, they fall far outside the scope of absolute protection. Even claims of qualified work-product protection are unlikely to succeed because the content does not reveal attorney thought processes and is not the result of legal research or case evaluation. The fact that these materials are transmitted to counsel, or used in litigation, does not cloak them in privilege where none otherwise exists.

Discovery: How to force production

To deal with social-media investigations effectively, you need to flush it out early and persistently by propounding discovery into the existence and scope of any such investigation.

Form interrogatories

13.1 requests all recorded statements, photographs, or video recordings of the incident or plaintiff. 13.2 asks for the identity of anyone who has examined or received these materials. Obtaining these responses in the plaintiff's initial set of discovery requests can be paramount in creating an initial timeline as to when defendants initiated a social-media investigation of your client. For example, if the defense retained an investigative service to conduct a social-media investigation shortly after the complaint was filed, it can be leveraged before the jury that the defense was more interested in attacking the plaintiff's credibility than investigating the facts of the case itself. This can be particularly compelling if the investigation was conducted before engaging in written discovery, depositions, or any meaningful fact-finding efforts.

Supplemental discovery

Use Code of Civil Procedure section 2030.070 to serve timely supplemental interrogatories. You get two before trial. Social-media investigations are often conducted by an investigative service as an ongoing observation of the plaintiff's social-media activity. Additional digital-surveillance reports, metadata logs, screenshots, and online activity summaries may be prepared near the time of defense medical examinations, depositions, or mediation so be sure to request strategically at various points in your case.

Expert discovery

Ask defense experts during deposition whether they reviewed digital-surveillance reports, or any other related materials. Defense experts who rely on these materials to form their opinions trigger further disclosure obligations under *Kennemur v. State of California* (1982) 133 Cal.App.3d 907.

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
July 2025

Deposition of the investigator: Exposing the cracks in the surveillance

If a third-party investigator prepared the defense's social-media report or surveilled your client, do not hesitate to depose them. When approached strategically, their testimony can be used to strengthen your client's case. The key is to neutralize the sting surveillance and expose the routine, impersonal, and often flawed nature of these investigations.

Identify and depose the investigator early

As previously noted, information regarding the identity of the surveillance vendors, individual investigators, and contact information can be obtained through Form Interrogatories 13.1 and 13.2, as well as specially tailored interrogatories directed at uncovering social media investigations. If defense refuses to disclose, file a motion to compel. Do not let surveillance remain a hidden tool.

Once the investigator or investigators are identified, serve deposition subpoenas for their testimony and reserve the right to introduce their videotaped depositions at the time of trial. (See Code Civ. Proc., § 2025.620.) This is an effective tactic to uncover the procedural missteps, bias, and lack of reliability in the underlying data.

Most investigators will not be well-prepared for an in-depth examination and often lack a full understanding of how their data may be used in litigation. Additionally, during the deposition, don't let the defense get away with making objections on behalf of the investigator as they do not have an attorney-client relationship nor is the investigator a party to the case.

Establish bias and financial incentive

Often, investigative services engaged by defense have a long-standing relationship with them that predates your client's case. Through the deposition testimony of the investigator, establish the ongoing relationship between investigator's employer and defense counsel. Get them to admit that the bulk of their assignments, if not all, come from the defense- side. Ask when they were retained, what instructions the defense gave them for the assignment, how they are compensated, whether they bill by the hour or per assignment, and how many files they have worked on for defense counsel's law firm. This testimony can help demonstrate to the jury that the investigator has a financial incentive to produce surveillance that aligns with the defense's narrative, rather than to provide an objective or unbiased account of your client's harm.

Emphasize the lack of context

Make the investigator acknowledge they had no medical records and have no idea what a "good day" versus a "bad day" looks like for your client. Get them to admit they do not know what symptoms of harm your client experiences or whether your client pushed through pain during activities depicted on social media.

Ask whether any of your client's social-media content contradicts the medical diagnoses or functional limitations outlined by treating physicians. Press the investigator on whether any of the posts depict activities that a doctor has expressly advised your client not to perform. If the investigator admits they have no understanding of what occurred before or after a given post, the credibility of their investigation begins to fall apart and appears more like speculation than reliable evidence.

Challenge the ethics and judgment behind the social-media investigation

Social-media investigations, while less visible than physical surveillance, can raise serious ethical concerns. Investigators claim to limit their investigation of the plaintiff to publicly available information or content legally accessible through proper channels, but this is not always the case, particularly when these investigations involve the review, collection, or archiving of content involving third parties like plaintiff 's family, friends, and professional contentions.

Ask whether the investigator actively searched through tagged posts, private group activity, or content posted by friends and family. Did they review or download photos of your client's children? Did they attempt to access private content without consent? Force them to acknowledge how much of their investigation involved third-party content or moments unrelated to your client's harm at issue in the case.

These questions shift the focus from your client to the conduct of the investigation itself, raising concerns about intrusion, overreach, and the ethics of combing through a person's personal life for litigation advantage.

Using video depositions to your advantage at trial

Since you noticed the investigator's videotaped deposition pursuant to Code of Civil Procedure section 2025.620, you may use it to your advantage at trial. Prepare page and line designations of the investigator's deposition for use in lieu of live testimony at trial. This will allow you to show the jury who the investigator was, what they were hired to do, how much they were paid, and how little they understood about your client, all without needing to bring the investigator into court or accommodate their schedule for trial.

Notice to produce at trial

Another tool to utilize in trying to obtain this material is by serving a notice to produce at trial under Code of Civil Procedure section 1987, subdivision (c), which "must be served at least 20 days before trial, or within any shorter period of time as the court may order, it may include a request that the party or person bring with him or her books, documents, electronically stored information, or other things."

It is important to request this evidence not only in discovery but also before trial as this may be another opportunity to inform the judge of defense tactics of trial by ambush if it wasn't produced in discovery and after being served with a notice to produce at trial. It is also important to remember that your notice to produce must be issued along with a notice to appear pursuant to section 1987(b).

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
July 2025

Be sure to state the exact materials you requested to show the judge that the specific item the defense seeks to use was requested repeatedly before trial to no avail. Things to request include "any and all videos taken by YOU of PLAINTIFF from the time of the incident through time of trial," and "All social media posts, photographs, comments, and messages that refer or relate to PLAINTIFF." You can adjust these to include requests for photographs, audio recordings, and any other sub rosa material.

Motions in limine: Preventing surprises at trial

Once you have obtained the materials related to the defense's social-media investigation, the next step is to ensure that no additional, undisclosed evidence from that investigation makes its way into trial. Any materials that were not properly disclosed during discovery should be excluded.

Your motion should attach and reference the defendant's verified discovery responses, clearly identifying what was produced, when it was produced, and what was withheld. The legal basis for exclusion should include Evidence Code section 352, emphasizing the court's discretion to exclude evidence when its probative value is substantially outweighed by the risk of undue prejudice, confusion, or surprise.

Courts have long recognized the importance of preventing trial by ambush. In *Thoren v. Johnson & Washer* (1972) 29 Cal.App.3d 270, 273, the court held that trial testimony and evidence may be excluded when it was omitted from responses to interrogatories. There, the court held that "one of the principal purposes of the Civil Discovery Act is to do away with the sporting theory of litigation – namely, surprise at trial." (*Id.* at 274.) The act of failing to disclose information in discovery "deprives [the] adversary of the opportunity of preparation which would disclose whether the witness will tell the truth and whether a claim based upon the witness' testimony is a sham, false or fraudulent." (*Ibid.*; see also, *Crumpton v. Dickstein* (1978) 82 Cal.App.3d 166, 170.)

Humanizing your client: Reframing social-media evidence through trial testimony

By the time of trial, you will likely know which social-media "hits" the defense intends to confront your client with. The most effective way to neutralize this tactic is not to contest the existence of the content, but to frame the jury's perception of it through your client's own words.

Direct testimony provides a critical opportunity to control the narrative. Use your client's testimony to show the contrast between isolated online moments and the day-to-day reality of life after injury. Your client does not need to deny the content, but merely contextualize it. A smiling photo, a brief family outing, or a casual post is an opportunity for your client to explain what is *not* shown. For example, the fatigue that followed, the medication required to get through the day, or the effort it took just to appear functional in that moment.

The preparation is key. Your client should be ready to explain any social-media presence with sincerity and humility. Acknowledging the post while offering truthful context shows credibility, not evasion. The jury does not expect perfection, but they do expect honesty.

Take control of your case before the defense does

In today's digital age, social-media investigations and video surveillance have become powerful tools in the defense's arsenal, capable of distorting facts and misleading juries with curated snapshots. Left unchecked, these tactics can erode a plaintiff's credibility and obscure the genuine harm suffered. But with proper education, strategic discovery, and proactive trial preparation, plaintiffs and their counsel can take control of the narrative before the defense defines it for them.

Investigative services may present social-media investigations as neutral fact-finding, but their purpose is often to undermine plaintiffs through selective and misleading digital fragments. The key is not simply to fight a defense-led social media investigation, but to reframe it. By understanding how these investigations are conducted, forcing timely production of all related materials, and preparing clients to thoughtfully address their online presence, you transform a potential liability into a manageable and even advantageous component of your case.

In doing so, you return the focus to where it belongs: the truth of your client's lived experience. Ultimately, at trial, the goal is to ensure jurors are not left with a still image, but the full human story behind it.

Garret Valerio is trial attorney at BD&J, PC *focusing on catastrophic injury, wrongful death, and product defect cases. He can be contacted via email at gv@bdj.com.*

Joseph Younes is a partner and trial attorney at BD&J, PC *in its wrongful-death and catastrophic-injury practice group. He has experience litigating a variety of cases, including large and complex personal injury, wrongful death, and product liability matters.*