Jamal Mahmood
JSM INJURY FIRM APC

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
July 2025

Navigating social media discovery for California plaintiffs

ETHICAL CONSTRAINTS AND PRACTICAL STRATEGIES FOR DEALING WITH THIS DOUBLE-EDGED SWORD

Discovery battles in the modern era often involve social media. Imagine defense counsel requests "All content from all of the plaintiff's social-media accounts from the past five years." How should you respond? Conversely, what if you suspect the defendant's Instagram is full of posts contradicting their story; how do you obtain those posts ethically and effectively? As plaintiff-side litigators, we must tread a fine line. We need to aggressively seek relevant online evidence to support our client's case (and anticipate what the defense might uncover), yet, also guard against improper privacy invasions and ensure our clients don't unwittingly destroy evidence.

This article provides guidance on preserving client social media, propounding and responding to social-media discovery, and abiding by ethical boundaries in the digital realm. The overarching theme is forethought and fairness: By acting early to secure important social- media data, crafting focused, lawful discovery requests, and respecting ethical limits, attorneys can harness the benefits of online information while avoiding common pitfalls.

Educate and preserve: The clients and their social media

As soon as litigation is reasonably anticipated, counsel must advise clients to preserve all relevant social-media content. Plaintiffs are often active on platforms like Facebook, Instagram, TikTok, Twitter (X), and YouTube – where posts, photos, or videos can either support or undermine legal claims.

The duty to preserve electronically stored information (ESI) in California arises when litigation is reasonably foreseeable. Violations can trigger serious consequences, even if unintentional. In one case, a school district faced issue and evidence sanctions for negligently deleting video footage after litigation became foreseeable, despite the absence of willfulness. (*Victor Valley Union High Sch. Dist. v. Superior Ct.* (2023) 89 Cal.App.5th 60.) The court rejected the safe harbor for routine ESI deletion because the duty to preserve had already attached.

The takeaway: Posts and accounts cannot be deleted or wiped once a dispute looms. California law allows a range of sanctions, such as monetary, issue, evidence, or even terminating sanctions, for misuse of the discovery process, including spoliation. (Code Civ. Proc., § 2023.030.) While harsh penalties like dismissal or default typically require willful misconduct, lesser offenses such as negligent spoliation, which may include a plaintiff deleting a Facebook post that contradicts an injury claim, can lead to adverse-inference instructions.

Practical tip: Issue a written litigation hold specifically addressing social media. Instruct the client, in unambiguous terms, to preserve all potentially relevant content. When in doubt, save it. Have them acknowledge this directive in writing. Explain that deleting posts after litigation is anticipated may be treated as spoliation. These steps help preserve evidence and shield both client and counsel from future claims of misconduct.

Can clients "clean up" their profiles?

Plaintiffs often want to remove embarrassing or irrelevant content once litigation begins. While it is ethically permissible to advise clients to adjust privacy settings, such as switching accounts to "private" or "friends only," it is not permissible to advise them to delete content. Even removing seemingly unrelated posts can trigger suspicions or result in the loss of potentially relevant material.

The safest approach is to preserve everything. If truly irrelevant but damaging content exists, discuss it transparently. In limited circumstances, removal from public view may be permissible, but only after a full archival copy is secured and relevance is ruled out. Disclosure of that removal may still be necessary to avoid claims of concealment.

Under California Rule of Professional Conduct 3.4(a), attorneys must not suppress evidence they are legally obligated to disclose. Instructing a client to delete relevant material risks violating Business & Professions Code section 6106 (moral turpitude) and section 6128(a) (deceit). In one notable case, a lawyer outside California who advised a client to "clean up" his Facebook was sanctioned over $500,000 and suspended. (*Allied Concrete Co. v. Lester* (2013) 285 Va. 295 [736 S.E.2d 699].)

Bottom line: Assume all content may be discoverable. Do not jeopardize the case – or your license – by altering or deleting social-media content. The consequences of spoliation almost always outweigh the embarrassment of disclosure.

Gathering social media from adverse parties and witnesses

When seeking social-media evidence from defendants or non-parties, start with public content. Reviewing publicly available posts is both ethical and part of a lawyer's duty of competence under California's standards (State Bar of Cal., Standing Com. on Prof. Responsibility & Conduct, Formal Opn. No. 2015-193 (2015).) Check platforms like Facebook, Twitter (X), LinkedIn, Instagram, TikTok, and YouTube for posts, photos, or videos tied to the case. Capture content early. Save as PDFs or screenshots with URLs and timestamps since users may delete or restrict access without notice. For dynamic feeds, consider web-capture tools that authenticate and timestamp content.

Ethical boundaries

California Rule 4.2 bars communicating with represented parties without their attorney's consent. This includes social-media friend or follow requests. Rule 8.4(c) prohibits deceit, such as using fake profiles or enlisting others to access private accounts. Such tactics are uniformly considered unethical and may render evidence inadmissible. Always treat

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
July 2025

online interactions as you would in person – honestly and transparently.

If a witness is unrepresented, you may contact them directly. If you choose to do so, you must identify yourself, explain your request, and accept a refusal if given. Anything more coercive risks ethical violations.

Caution with jurors

While reviewing a juror's public profile is generally permitted, you may not engage, follow, or trigger any alert that notifies them of your activity (e.g., LinkedIn views). Always comply with court instructions and err on the side of caution when conducting juror research.

Propounding focused social-media discovery

If publicly available social media content is insufficient, request private content through formal discovery, typically via requests for production (RFPs) or interrogatories. Avoid vague demands like "produce your entire Facebook history," which invite objections and are rarely upheld. Courts expect narrowly tailored, relevant, and proportional requests, especially for social media.

Use precise, focused language

Frame RFPs to target relevant time periods and subject matter:

- *Personal injury:* "All photographs, videos, or social media posts depicting plaintiff engaging in physical activities from the date of the accident to present."
- *Employment/emotional distress:* "All social media posts or messages from June 2022 to December 2022 referencing plaintiff's employment at XYZ Corp., termination, or emotional state."

Requests like these are easier to justify and defend than broad five-year account history demands.

Identify accounts early

Use interrogatories to uncover all platforms and usernames used in the past five years. Once identified, you can follow up with platform-specific RFPs. Don't overlook private-messaging platforms (e.g., WhatsApp or DMs), which may contain relevant content, albeit with heightened privacy considerations.

Two-stage approach

Some courts require a threshold showing of relevance before compelling private content. For instance, a public post of a plaintiff rock climbing post-injury might justify requesting additional private posts of similar activities. Without such a showing, courts are unlikely to compel broad access. In *Mailhoit v. Home Depot U.S.A., Inc.* (C.D.Cal. 2012) 285 F.R.D. 566, the court addressed the scope and limits of social-media discovery under the Federal Rules of Civil Procedure, and held that discovery was limited to content directly relevant to the plaintiff's emotional distress, thereby limiting wholesale production.

Show good faith

If the opposing party resists, propose compromises such as allowing them to self-search for keywords or produce posts tied to specific injuries or events. This demonstrates reasonableness and helps justify a motion to compel if needed.

No subpoenas to social-media platforms

You cannot subpoena Facebook, Twitter, or Instagram for a user's content. The federal Stored Communications Act (SCA) (18 U.S.C. §§ 2701–2712 (2023)) prohibits service providers from disclosing private user data in civil cases. California courts have affirmed that discovery laws cannot override the SCA.

Practice tips:

- If seeking production, be prepared to explain that the SCA prevents direct subpoena to the platform, hence the request must go through the user.
- If resisting a broad request, use the SCA to argue that opposing counsel is not entitled to login credentials or full account downloads. Counsel – not the opponent – should review and produce responsive content.

Lawful workarounds under the SCA

Although the Stored Communications Act bars subpoenas to social media providers, there are several legitimate ways to obtain content:

- User consent: A party can voluntarily download and produce their own social media archive (e.g., via Facebook's data download feature). Courts can order this and limit production to relevant portions.
- Authorized third parties: Content can be obtained from someone with lawful access, such as a friend or witness who received a message or screenshot. This is permissible, so long as it's done without coercion or violation of platform terms.
- In camera review: Courts may order a private review of the entire account by a judge or special master. Only relevant material is then disclosed. This balances discovery needs with the user's privacy rights – particularly important under California's constitutional right to privacy.

If opposing counsel objects to production or raises privacy concerns, proposing in camera review as a compromise often demonstrates reasonableness and may help avoid discovery disputes.

Responding to social-media discovery requests: Protecting your client

When your client receives a sweeping request for social media, don't panic and don't allow a digital fishing expedition. The California Constitution protects individual privacy, including on social media. (Cal. Const., art. I, § 1.) That right is qualified, not absolute, and courts evaluate it using a balancing test: Discovery must be directly relevant and reasonably necessary to override privacy objections.

A lawsuit doesn't open the door to a litigant's entire social-media history. The requesting party must show that specific content is likely to be relevant. Vague or overbroad requests are likely to fail under this standard.

Best practices for responding

- Work with your client to identify and collect only relevant content. Use keyword or date-range searches to locate posts connected to the incident (e.g., injury, emotional distress).
- Review content together and produce responsive, non-privileged material.
- If posts are sensitive but arguably responsive (e.g., messages involving unrelated personal issues), consider redacting or logging them. California

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
July 2025

case law supports redaction of irrelevant private details. (*Britt v. Superior Ct.* (1978) 20 Cal.3d 844.)

• Document withheld items with a simple privacy or privilege log, e.g., "Private message with spouse, dated X, unrelated to the incident – withheld based on privacy."

Refusing overreach

If opposing counsel demands passwords, full account downloads, or forensic imaging, you can object. Cite the SCA (which prohibits indirect access via the user), California's privacy protections, and Code of Civil Procedure section 2017.020, which limits discovery that is overly intrusive. Offer narrower alternatives: "We'll produce posts about the injury but not grant unrestricted account access."

Courts often find a middle ground and order keyword-based production or protective orders (e.g., "attorneys' eyes only") to limit exposure of sensitive content.

Stay reasonable and transparent

Where appropriate, offer factual stipulations to avoid unnecessary disclosures. For example: "Plaintiff confirms they took a hiking trip in June 2023." It may not satisfy all demands, but it shows good faith and narrows disputes.

Finally, document your efforts in your responses. Clearly state what was searched, what was produced, and what was withheld with justification. For example: "Plaintiff has produced all Facebook posts from May–December 2022 referencing her back injury or physical activity. Posts unrelated to those topics have been withheld as private and irrelevant."

Such transparency can preempt discovery disputes and demonstrate to the court that your client acted responsibly and cooperatively.

Handling and authenticating social-media evidence

In complex cases, especially those involving large volumes of social-media content or where authenticity may be challenged, it's worth engaging an e-discovery expert. Forensic tools like X1 Social Discovery and PageVault are designed to collect social-media data in a defensible manner, preserving metadata and generating evidentiary reports.

These tools can download full profiles, message threads, and videos, and can filter by keyword or date range, which is particularly helpful if the court limits the scope of production. The key advantage is twofold: comprehensive capture of relevant content and stronger admissibility. Vendors can testify or provide affidavits authenticating the data and confirming the integrity of the collection process, which is critical when introducing social media evidence in court.

In California, as elsewhere, authentication is essential. (Evid. Code, §§ 1400–1401.) Courts expect counsel to lay a proper foundation. Someone must attest that a screenshot or message is a true and accurate representation of what was posted online, and, where necessary, that the content came from the party's account. A forensic collection supports this by establishing a clear chain of custody and verifying technical details such as timestamps or hash values.

To avoid later disputes, keep a contemporaneous record of how and when the content was obtained. Printouts should note the URL and date of access; downloaded media should be preserved in original format with its source documented. If authenticity is later questioned, this kind of preparation allows you to rebut claims that a post was fabricated or altered.

Courts are becoming more familiar with social-media evidence, but continue to expect diligence in authentication. A strong collection process – supported by expert analysis if needed – can help ensure critical content is admitted without dispute. Plan ahead so key evidence isn't excluded on technical grounds.

Monitoring social media during litigation

Parties often remain active online throughout the years-long process of litigation. Thus, social-media monitoring shouldn't end after initial discovery. New posts may surface that impact damages, credibility, or even the enforceability of a settlement. We've all seen examples: A plaintiff claiming serious injury shares vacation photos or celebrates a settlement online in violation of a confidentiality clause. In one real case, a plaintiff posted, "Finally settled, time to party!" prompting the defense to argue she breached confidentiality, jeopardizing the agreement. Defendants, too, may post reckless comments about the lawsuit or judge, which can be used for impeachment.

To stay ahead, set up Google Alerts for party names, and periodically check public profiles. Following public accounts without engaging or bypassing privacy settings is generally permissible. If a post appears to violate a court order or contains new, material facts, such as evidence of a new injury source, preserve it and consider notifying opposing counsel or the court as appropriate.

Just as important is advising your own clients. They need to understand that social media content created during litigation can be used against them. Even innocent posts can be misinterpreted. A smiling photo may undercut a claim of emotional distress, or a gym check-in may cast doubt on an injury claim. While you cannot instruct a client to lie or hide existing evidence, you should strongly discourage them from posting anything that could later become problematic. A practical way to explain it is: "Assume the defense is reading everything you post. If you wouldn't want to see it quoted in court, don't post it." This isn't about suppressing truth but about preventing the creation of new evidence that could harm the case. It's no different than advising a client not to talk about the lawsuit publicly or provoke the other side online. It's sound legal strategy and an important part of client protection.

Dealing with social-media spoliation or abuse by the other side

Even with careful planning, you may face an opponent who destroys or conceals social-media evidence. A defendant might delete posts after being

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
July 2025

served, or a witness may wipe an account following a subpoena. If you suspect spoliation, act quickly. As previously mentioned, California law offers remedies through California Code of Civil Procedure section 2023.030, which authorizes sanctions ranging from monetary penalties to evidence, issue, or even terminating sanctions in serious cases.

The severity of any sanction depends on intent and prejudice. Although loss of electronically stored information (ESI) resulting from the routine, good-faith operation of an electronic information system may be protected (see Code Civ. Proc., § 2031.060(f)), manually deleting relevant content after a duty to preserve arises is not.

If you believe key evidence was deleted, consider requesting a court order for forensic inspection or limited subpoena of non-content records, such as account deactivation dates or login history. While the Stored Communications Act (SCA) bars providers from disclosing content, they may confirm when an account was deactivated which is helpful if a deletion coincided with the litigation timeline.

California does not recognize an independent tort for spoliation, so the remedy lies within the litigation process. (See *Cedars-Sinai Med. Ctr. v. Superior Ct.* (1998) 18 Cal.4th 1.) Per the California Civil Jury Instructions, courts may instruct juries to draw adverse inferences, and permit such findings, where evidence was willfully destroyed. Intentional deletion with prejudice to the opposing party supports the harshest sanctions, while even negligent spoliation may result in lesser penalties, as in cases where courts imposed issue sanctions for the negligent loss of surveillance video after the duty to preserve had attached.

If your client is accused of spoliation, be ready to show your preservation efforts. Documentation matters. Provide a declaration outlining steps taken to retain and produce relevant social media, including litigation hold notices and archived content. While deletion can sometimes be innocent, the appearance of misconduct can be just as damaging. The best defense is proactive diligence and a clear, verifiable record of preservation.

Privacy vs. discovery: The balancing act

It's natural for plaintiffs to feel uneasy about handing over personal social media content, especially when it was privately shared and only intended for their "friends." But once litigation begins, relevant content – even if posted privately – may need to be disclosed. California's constitutional right to privacy is not absolute.

When a plaintiff places a matter at issue, courts will compel disclosure of information directly related to that issue, while aiming to limit unnecessary intrusion. As the California Supreme Court recognized in *Williams v. Superior Ct.* (2017) 3 Cal.5th 531, 557, privacy protections must yield when disclosure is reasonably calculated to lead to the discovery of admissible evidence, provided the request is narrowly tailored and the intrusion justified. Privacy objections don't block discovery but can help ensure it is appropriately limited and subject to safeguards.

Counsel should use available tools to protect client privacy. Courts often permit redactions of unrelated personal content or designate materials as "Confidential" under protective orders. For particularly sensitive material, in camera review or limitations on dissemination may be appropriate. For example, if physical capacity is in dispute, photos of the plaintiff engaging in physical activity are likely discoverable, whereas unrelated images, such as those from a family gathering, generally are not. California courts consistently hold that only content directly relevant and necessary to the litigation must be produced.

Clients should be prepared for the possibility that some personal content will be seen by the opposing side. Clear, early communication helps manage expectations. Emphasize to your client that your role as their attorney is to protect their dignity and limit irrelevant disclosures, while ensuring that genuinely relevant facts are produced appropriately. This not only reassures clients but also encourages them to be more cautious with their online activity throughout the case.

Conclusion

Social media is a double-edged sword in litigation: It is capable of strengthening your client's case or cutting it down. It can offer compelling evidence to corroborate claims or impeach an adversary, yet it also brings risks: privacy intrusion, reputational harm, and spoliation pitfalls that can seriously damage a case. California plaintiffs' attorneys must approach this landscape with both diligence and ethical restraint.

If attorneys can advise clients early on to preserve their social media and practice responsible online behavior, coupled with precise discovery requests and objections, as well as the right tools to collect and authenticate data, they can transform social media from a liability into a strategic asset.

From the outset, treat social media with the same weight as physical evidence or key records: Investigate it, secure it, request it, and produce it thoughtfully.

Equally important is knowing where the ethical boundaries lie and keeping well within them. The credibility you build by handling social media conscientiously will serve you when presenting that crucial Instagram post or Facebook message in court. With sound practices, social media can help you construct a persuasive, evidence-based narrative while avoiding the pitfalls that have derailed others.

Jamal S. Mahmood is the founder of JSM Injury Firm APC, *representing plaintiffs in catastrophic injury, wrongful death, auto accident, and premises liability cases in California. He holds a B.A. from the University of Oregon and graduated magna cum laude from Western State College of Law. He can be reached atjamal@jsminjuryfirm.com.*