HOW TO GET SOCIAL MEDIA EVIDENCE ADMITTED INTO COURT

Admitting social media and deep web findings into evidence is not difficult, but it does require ethical considerations and prompt action. You need to ensure that you have:

- Verified the creation and ownership of the content with a witness,
- Collected and preserved the content promptly and ethically to safeguard against deletions and alterations,
- Gathered relevant electronic device records that correspond to the social media content,
- Maintained a flawless chain of custody of the evidence.

In a recent New York Court of Appeals case (People v. Mayo), the lower court unsuccessfully attempted to admit a photograph downloaded from Facebook, alleging the photo belonged to the defendant and depicted the defendant wearing similar clothing worn by the perpetrator. Because the photo was not properly authenticated and the only testimony about the photograph was provided by a police witness who had searched for the Facebook profile one and a half years after the crime, the court ruled not to admit the photo into evidence. Additionally, the People were unable to establish the owner and controller of the photo and therefore could not prove that the photo had been altered.

What can we learn from the People v. Mayo?

Proper Authentication:
Authenticity can come in many forms. In this case, the defendant recalling and claiming ownership of the photograph obtained from Facebook could aid in validating the evidence. But there's an even more secure way to authenticate social media evidence: collecting and preserving content using metadata and source code. Every photograph posted to Facebook contains metadata, or data that is embedded within the photo. Metadata can tell us where the photo was taken, when it was taken, and the size of the file. The source code is a programming language that preserved the content as it was found originally on a posted page and remains consistent despite alterations that may be made to a person's accounts.

Ethically Collected and Preserved:
It's not enough to find and download evidence from social media profiles and the web. Collecting evidence requires discretion to protect the chain of custody and adherence to the best evidence rule. Algorithms used on websites and social media profiles can alert subjects about your investigation of their public accounts. Connecting with subjects through "friending" can expose you and your firm to vulnerable data breaches. Collecting evidence improperly can suggest that you may have altered, concealed, or falsified online evidence.

Prompt Action:
Chances are, if you're looking for social media evidence, the opposition is looking to social media for evidence, too. Once social media posts and profiles are deleted, they're gone. Acting quickly and discreetly is the only way to ensure you can collect and preserve the evidence you need.

Who You Gonna Call?

SMI Aware is the leader in ethical discovery, collection, and preservation of information from social media and open-sources online. Our proprietary software and certified analysts preserve evidence in compliance with legal ethics rules allowing us to secure the chain of custody of evidentiary content like images in our investigations. We help legal professionals find and authenticate scope-driven data in comprehensive reports that are defensible in the court of law.