Social Media Content and E-Discovery

A guide to competently obtaining and preserving evidence.

BY CRAIG BALL

Social media content, or SMC, is a rich source of evidence. Photos and posts shed light on claims of disability and damages, establish malicious intent, and support challenges to parental fitness—to say nothing of criminals who post selfies at crime scenes or holding stolen goods, drugs, and weapons. SMC may expose mental instability, propensity to violence, hate speech, racial animus, or misogyny. SMC is increasingly a medium for business messaging and the primary channel for cross-border communications. In short, SMC and messaging are heirs-apparent to email in their importance to e-discovery.

Competence demands swift identification and preservation of SMC.

Screenshots of SMC are notoriously unreliable, tedious to collect, and inherently unsearchable. Applications like X1 Social Discovery and service providers like Hanzo can help with SMC preservation, but the task demands little technical savvy and no specialized tools. Major SMC sites offer straightforward ways users can access and download their content. Armed with a client's login credentials, lawyers, too, can undertake the ministerial task of preserving SMC without greater risk of becoming a witness than if they'd photocopied paper records.

Collecting Your Client's SMC

Collecting SMC is a two-step process of requesting the data followed by downloading. Minutes to hours or longer may elapse between a request and download availability. Having your client handle collection weakens the chain of custody; so, instruct the client to forward download links to you or your designee for collection. Better yet, do it all yourself.

Obtain your client's user ID, password for each account, and written consent to collect. Instruct your client to change account passwords for your use, re-enabling customary passwords following collection. Clients may need to temporarily disable two-factor account security. Download data promptly as downloads are available briefly.

Collection Steps for Seven Social Media Sites

Facebook: After login, go to *Settings >Your Facebook Information>Download Your Information*. Select the data and date ranges to collect (e.g., Posts, Messages, Photos and Videos, Comments, Friends, etc.). Facebook will email the account holder when the data is ready for download (from the *Available Copies* tab on the user's *Download Your Information* page). Facebook also offers an *Access Your Information* link for review before download.

Twitter: After login, go to *Settings and privacy>Your Twitter data>Download your Twitter data*. Re-enter the password and choose *Request Archive*. Twitter will email the account holder when a compressed file holding the data is ready for download. Twitter permits one archive retrieval a month.

Google: Go to *https://accounts.google.com*, select *Use Another Account* and log in to client's account. Choose *Data & personalization>Download your data*. Select data to include (be sure your client has expressly authorized collection) and the archival format (e.g., zip). Google will email the account holder when a compressed file holding the data is ready for download.

Instagram: Log in and go to the user's profile. Select the gear icon (*Settings*), then *Privacy and Security>Request Download*. The data will be in JSON format inside a compressed file. Once decompressed, it can be viewed using any free online JSON parser.

LinkedIn: Log in and select *Me>Settings & Privacy*. Under the *Privacy* tab, choose *Getting a copy of your data* and the specific data sought. If uncertain, choose *Download larger data archive*. Click *Request archive*.

Snapchat: Log in at *https://accounts.snapchat.com* and select *My Data>Submit Request*.

Tumblr: Log in and select *Account> Settings>Privacy>Request Privacy Data*. The downloaded data will be in a compressed file in JSON format.

Review and Authentication

SMC is often voluminous and encoded in unfamiliar formats like JSON. So, as with other information collected in e-discovery, the competent way to index, search, review, and tag electronic evidence is by use of e-discovery review tools, e.g., Relativity, iCONECT, Logikcull, Everlaw.

Though not essential, it's prudent to calculate a hash value for preserved SMC to demonstrate its integrity.[1] A hash value is a digital fingerprint of data. If the hash value obtained when the data was collected matches the hash value when used, the data is demonstrably unchanged. Many hashing tools can be downloaded online at no cost.

Caveat: There are no "guest passes" to social media accounts. When you log in as the account holder, you stand in the account holder's shoes. Keep good records of access and note what you did while logged in. Likewise, never seek or consent to access an opponent's social media account using opponent's credentials or you open yourself up to claims that you added or altered content. **TBJ**

Note

1. *See, e.g.*, Fed. R. Evid. 902(13) & (14).

CRAIG BALL
is a trial attorney in Texas and an adjunct professor at the University of Texas School of Law, where he teaches electronic evidence and digital discovery. He focuses on digital forensics, e-evidence, visual persuasion, and electronic discovery and limits his practice to service as a court-appointed special master and consultant in electronically stored information. Ball is the 2019 recipient of the State Bar of Texas Gene Cavin Award for Lifetime Achievement in Continuing Education.