Overcoming Potential Legal Challenges to the Authentication of Social Media Evidence

Overcoming Potential Legal Challenges to the Authentication of Social Media Evidence

By John Patzakis[1]

Summary:

Social media evidence is highly relevant to most legal disputes and broadly discoverable, but challenges lie in evidentiary authentication without best practices technology and processes. This whitepaper examines these challenges faced by eDiscovery practitioners and investigators and illustrates best practices for collection, preservation, search and production of social media data. Also highlighted in this paper are examples of numerous unique metadata fields for individual social media items that provide important information to establish authenticity, if properly collected and preserved.

With about 1.3 billion Facebook users and 500 million people with Twitter accounts, evidence from social media sites can be relevant to just about every litigation dispute and investigation matter. Social media evidence is widely discoverable and generally not subject to privacy constraints when established to be relevant to a case, particularly when that data is held by a party to litigation or even a key witness. However recent court decisions reflect that the main pressing concern for attorneys, eDiscovery practitioners and investigators is the authentication of social media data for admission into evidence in court.

Under US Federal Rule of Evidence 901(a), a proponent of evidence at trial must offer "evidence sufficient to support a finding that the matter in question is what its proponent claims." Unless uncontroverted and cooperative witness testimony is available, the proponent must rely on other means to establish a proper foundation. A party can authenticate electronically stored information ("ESI") per Rule 901(b)(4) with circumstantial evidence that reflects the "contents, substance, internal patterns, or other distinctive characteristics" of the evidence. Many courts have applied Rule 901(b)(4) by ruling that metadata and file level hash values associated with ESI can be sufficient circumstantial evidence to establish its authenticity.[2]

Given the transient and cloud-based nature of social media data, it generally cannot be collected and preserved by traditional computer forensics tools and processes. Full disk images of computers in the cloud is effectively impossible and the industry has lacked tools designed to collect social media items in a scalable manner while supporting litigation requirements such as the capture and preservation of all key metadata, read only access, and the generation of hash values and chain of custody. In fact, the proper and timely preservation of social media evidence is a major concern, with courts finding spoliation or disallowing mere printouts of social media data as inadequate to establish a proper foundation.[3]

In *State of Connecticut v. Eleck,*[4] the court rejected Facebook evidence in the form of a simple printout, for failure of adequate authentication. The court noted that it was incumbent on the party to seeking to admit the social media data to offer detailed "circumstantial evidence that tends to authenticate" the unique medium of social media evidence. Conversely, in *State v. Tienda,*[5] the prosecution successfully admitted key MySpace evidence over the defendant's objection, laying a foundation through various circumstantial evidence. Among this key circumstantial evidence were relevant metadata fields, other evidence from defendant Tieda's MySpace page, including his username, which was consistent with Tienda's commonly known nick name, his email addresses registered to the account, user ID number, stated location (Dallas), communications with other suspects, and numerous posted photos of Tienda with associated date and time stamps.

The Texas appellate court determined that "this is ample circumstantial evidence—taken as a whole with all of the individual, particular details considered in combination—to support a finding that the MySpace pages belonged to the appellant and that he created and maintained them." Similarly, a Delaware court, finding that social media evidence was no different from any other evidence and that it was thus subject to the same authentication test as any other exhibit, applied the test set forth in *Tienda*, which has become the majority view in the U.S. The Delaware court determined that Facebook messages in that case were properly authenticated based upon the victim's testimony, and circumstantial evidence in the form of metadata, including date stamps, and user account names.[6]

The lesson from these cases illustrates that to properly address these authentication and preservation challenges, social media data must be properly collected, preserved, searched and produced in a manner consistent with best practices so that all available circumstantial evidence is collected, including metadata. When social media is collected with a proper chain of custody and all associated metadata is preserved, authenticity is much easier to establish. For instance, the following are just some of the key metadata fields for individual Facebook posts (such as a photo or status update) that together provide important information to establish authenticity of the tweet, if properly collected and preserved:

Metadata Field	**Description**
Uri	Unified resource identifier of the subject item
fb_item_type	Identifies item as Wallitem, Newsitem, Photo, etc.
parent_itemnum	Parent item number-sub item are tracked to parent
thread_id	Unique identifier of a message thread
recipients	All recipients of a message listed by name
recipients_id	All recipients of a message listed by user id
album_id	Unique id number of a photo or video item
post_id	Unique id number of a wall post
application	Application used to post to Facebook (i.e, from an iPhone or social media client)
user_img	URL where user profile image is located
user_id	Unique id of the poster/author of a Facebook item
account_id	Unique id of a user's account
user_name	Display name of poster/author of a Facebook item
created_time	When a post or message was created
updated_time	When a post or message was revised/updated
To	Name of user whom a wall post is directed to
to_id	Unique id of user whom a wall post is directed to
Link	URL of any included links
comments_num	Number of comments to a post
picture_url	URL where picture is located

Any one or combination of these fields can be key circumstantial data to authenticate a social media item, or constitute substantive evidence in and of itself. Twitter and LinkedIn items have their own unique but generally comparable metadata[7]. In addition to collection of all such key metadata, it is important that MD5 hash values of each social media item are automatically generated at the time of their collection, and that unique case information is generated to support a proper chain of custody. However, many ad hoc measures currently used to collect social media for use in court do not meet these requirements. Screen capture tools and many archive services fail to collect most available metadata or generate hash values for individual social media items upon collection.

The Facebook self-collection mechanism currently will not collect most available metadata information, will not generate hash values, and will only provide content from the user's own account while omitting content contributed by that user to their friend's account, such as their "walls." eDiscovery leader KMPG provided a written release noting that the Facebook download feature "was not conceived to be a forensic collection tool. The only original timestamps that it preserves are in the HTML files which can be easily modified." There currently is no self-collection or even export feature for Twitter.

The Maryland Supreme Court in *Griffin v. State* prognosticated that to address the compelling requirement to authenticate social media evidence, methods and technologies for authenticating social media data likely will develop "as the efforts to evidentially utilize information from [social networking] sites increases." [8] To answer this call, X1 Social Discovery is one such new technology now available to the legal and eDiscovery community.

X1 Social Discovery establishes a defensible chain of custody through several functions. MD5 hash values of individual social media items are calculated upon capture and maintained through export. Automated logging and reports are generated. Key metadata unique to social media streams are captured through deep integration with APIs provided by the leading social media sites.[9] This functionality is provided along with a very scalable workflow and instantaneous search results. Tens of thousands of social media items can be captured per hour and then quickly searched, reviewed and exported in support of a traditional investigative and eDiscovery process. The speed, scalability and ease of use of X1 Social Discovery coupled with its best-practices preservation and chain of custody data capabilities now provides legal and eDiscovery professionals the means to finally address the universe of social media evidence on a very routine basis.

Notes:

[1] John Patzakis is an attorney who frequently lectures and is extensively published on issues related to computer forensics, electronic discovery and the authentication of electronically stored information. He is the Founder and CEO of X1. www.x1.com.
Previous to X1, he was a co-founder of Guidance Software, Inc., the developer of EnCase.

[2] *Lorraine v. Markel American Insurance Company*, 241 F.R.D. 534 (D.Md. May 4, 2007)

[3] *Lester v. Allied Concrete Company* (VA, 2011) is believed to represent the largest eDiscovery sanction ever imposed on an individual attorney (see http://wp.me/p1R4t2-49 for case details). See also, *Katiroll Co., Inc. v. Kati Roll & Platters, Inc.*, 2011 WL 3583408 (D.N.J. Aug. 3, 2011)

[4] 2011 WL 3278663 (Conn.App. 2011)

[5] 5 358 S.W.3d 633 (Tx.App.2012);

[6] *Parker v. State*, 2014 WL 621289 (De. App 2014)

[7] *Barnes v. CUS Nashville*, LLC, 2010 WL 2265668 (M.D. Tenn. 2010)

[8] *Griffin v. State of Maryland*, 2011 WL 1586683, at *94 (Md. 2011)

[9] A full listing of metadata captured from Twitter by X1 Social Discovery is available here (X1 blog): http://wp.me/p1R4t2-1W and the product user manual: http://download.x1discovery.com/cs/x1sd_user_manual.pdf

X1 delivers next generation eDiscovery for social media, cloud and the enterprise. Built upon the market leading X1 search solution, X1 provides a ground-breaking platform for social media eDiscovery and supports investigations of cloud-based data.

For more information, please contact
info@x1.com

X1 Discovery, Inc.
130 West Union Street, Pasadena, CA 91103

877-999-1347 tel
626-535-2701 fax