Consilio / ADVANCED LEARNING INSTITUTE

Consilio Institute: White Paper

GONE VIRAL: SOCIAL MEDIA IN EDISCOVERY

By Matthew Verga, Esq.
Director of Education

Consilio Institute: White Paper

GONE VIRAL: SOCIAL MEDIA IN EDISCOVERY

TABLE OF CONTENTS

Disclaimers

The information provided in this publication does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in this publication are provided for general informational purposes only. While efforts to provide the most recently available information were made, information in this publication may not constitute the most up-to-date legal or other information.This publication contains links to third-party websites. Such links are only for the convenience of the reader; Consilio does not recommend or endorse the contents of the third-party sites.

Readers of this publication should contact their attorney to obtain advice with respect to any particular legal matter. No reader of this publication should act or refrain from acting on the basis of information in this without first seeking legal advice from counsel in the relevant jurisdiction. Only your individual attorney can provide assurances that the information contained herein – and your interpretation of it – is applicable or appropriate to your particular situation.

Use of this publication, or any of the links or resources contained within, does not create an attorney-client relationship between the reader and the author or Consilio. All liability with respect to actions taken or not taken based on the contents of this publication is expressly disclaimed. The content of this publication is provided "as is." No representations are made that the content is error-free.

GONE VIRAL: SOCIAL MEDIA IN EDISCOVERY

As a review of almost any day's news will demonstrate, social media remains an influential, indispensable part of life – for better or for worse. Our usage of social media has grown dramatically over the past sixteen years[1]:

When Pew Research Center began tracking social media adoption in 2005, just 5% of American adults used at least one of these platforms. By 2011 that share had risen to half of all Americans, and today 72% of the public uses some type of social media.

Our high rate of usage has continued, without abatement, "[d]espite a string of controversies and the public's relatively negative sentiments about aspects of social media"[2] [internal hyperlinks omitted]. And, our rate of creation of new materials on these platforms continues to grow each year[3]:

Social Media in eDiscovery

As social media has been working its way ever deeper into our relationships, our professional activities, and our culture as a whole, its impact on discovery has been growing as well:

- The Advisory Committee Notes to the FRCP's December 2015 Amendments[4] include an explicit reference to the need to understand and consider social media sources during preservation: "It is important that counsel become familiar with their clients' information systems and digital data — including social media — to address these issues."
- As social media communication channels (and smartphones) have become more frequent discovery sources, so too have emoji shown in more cases. In 2018, Santa Clara University law professor Eric Goldman published Emojis and the Law[5] in the Washington Law Review, and revealed his case survey results showing[6] that, "[b]etween 2004 and 2019, there was an exponential rise in emoji and emoticon references in US court opinions, with over 30 percent of all cases appearing in 2018."
- In February 2019, in recognition of these growing impacts, the Sedona Conference published a Second Edition of its Primer on Social Media[7] to help practitioners meet the eDiscovery challenges posed by social media evidence: ". . . traditional social media platforms . . . have created preservation, production, and evidentiary challenges that counsel should learn to recognize and address."
- In April 2019, the International Legal Technology Association published the results of its 2018 Litigation and Practice Support Survey,[8] revealing that 90% of responding professionals (overwhelmingly from law firms) had handled at least one case involving the collection and processing of social media data in the prior year, a 7% increase over the prior year.[9] Moreover, 19% reported handling more than 20 such cases, a 46% increase over the prior year.

[1] *Social Media Factsheet, PEW RESEARCH CENTER, https://www.pewresearch.org/internet/fact-sheet/social-media/ (Apr. 7, 2021).*
[2] *Brooke Auxier and Monica Anderson, Social Media Use in 2021, PEW RESEARCH CENTER, https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/ (Apr. 7, 2021).*
[3] *Lori Lewis, Infographic: What Happens In An Internet Minute 2021, ALL ACCESS, https://www.allaccess.com/merge/archive/32972/infographic-what-happens-in-an-internet-minute (Apr. 13, 2021).*
[4] *Fed. R. Civ. P. 37 advisory committee's note, available at https://www.law.cornell.edu/rules/frcp/rule_37.*
[5] *Eric Goldman, Emojis and the Law, 93 WASH. L. REV. 1227 (2018), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3133412.*
[6] *Dami Lee, Emoji are showing up in court cases exponentially, and courts aren't prepared, THE VERGE, https://www.theverge.com/2019/2/18/18225231/emoji-emoticon-court-case-reference (Feb. 18, 2019).*
[7] *The Sedona Conference, Primer on Social Media, 20 SEDONA CONF. J. 1 (2019), available at https://thesedonaconference.org/publication/Primer_on_Social_Media.*
[8] *Cindy MacBean, 2018 Litigation and Practice Support Survey Results, ILTA (Apr. 2019), available at http://epubs.iltanet.org/i/1108621-lps19/36?_ga=2.231156186.434461956.1629978821-1135214194.1629978821.*
[9] *ILTA's 2017 Litigation and Practice Support Technology Survey Results, ILTA (Apr. 2018), available at http://epubs.iltanet.org/i/973671-lps18/55?_ga=2.39038435.1141759458.1531162513-441756871.1531162513.*

About this White Paper

In this white paper, we will review the things practitioners need to know about dealing with social media in eDiscovery, including: what sources there are, what data those sources contain, how reliable it is, how it can be obtained, how it can be authenticated, and how courts have responded to its spoliation.

SOCIAL MEDIA SOURCES

Although there are numerous social media services, the vast majority of use activity is centered on a few dominant services. According to the Pew Research Center's April 2021 Social Media Fact Sheet,[10] these ten services will be your most likely social media sources:

- **YouTube** – used by 81% of US adults – focused on sharing, watching, and commenting on recorded and live-streamed video content
- **Facebook** – used by 69% of US adults – site on which users create personal profiles, add friends, send messages, post status updates, share media and links, read articles, chat with others, join groups, stream live video, and more
- **Instagram** – used by 40% of US adults – site, owned by Facebook, focused on sharing and commenting on users' photos and videos
- **Pinterest** – used by 31% of US adults – focused on creating and sharing "pinboards" of favorite or themed images and videos, both uploaded and collected from the Internet
- **LinkedIn** – used by 28% of US adults – focused on professional networking and job seeking, with profiles akin to resumes and a variety of industry-specific groups to join
- **Snapchat** – used by 25% of US adults – private, ephemeral[11] social site on which users share photos, videos, and stories that disappear after a designated amount of time
- **Twitter** – used by 23% of US adults – focused on rapid, chronological sharing of brief messages called "tweets," each of which is no more than 280 characters in length
- **TikTok** – used by 21% of US adults – focused on creating, sharing, and viewing short videos
- **Reddit** – used by 18% of US adults – topical discussion forums in which news and posts are socially-curated (*i.e.*, user up-votes and down-votes determine ranking/visibility)
- **Nextdoor** – used by 13% of US adults – focused on connecting small networks of actual neighbors to share neighborhood news and local service provider information

Among the users of these social media sites, many use the sites daily, including: 70% of Facebook users, 59% of Instagram and Snapchat users, 54% of YouTube users, and 46% of Twitter users.

[10] *Social Media Factsheet, PEW RESEARCH CENTER, https://www.pewresearch.org/internet/fact-sheet/social-media/ (Apr. 7, 2021).*
[11] *Ephemeral social media communications have added functionality that automatically deletes them after they have been read or after a short period of time specified by either the platform or the sender.*

WHAT'S THERE

Social media services typically incorporate multiple forms and formats of media and communication together, creating a complex source of diverse ESI. Facebook, for example, allows sharing of photos and videos, status updates, public posts, private messages, live chats, video streams, and more. Twitter, too, accommodates the uploading of a variety of multimedia file types, along with a combination of public posts, private messages, and live streams.

In addition to the material posted and uploaded by users, social media services also record extensive information[12] about each user's activities on the service, such as what content they've liked or shared, logs of when and how they've accessed the service, and sometimes more. For example, it was revealed in 2018[13] that Facebook accounts might also contain years' worth of call and messaging logs (including details like when, for how long, and with whom) for users who accessed Facebook from their Android smartphones.

All of this material accumulates rapidly into large volumes, because as noted above, social media users access these services frequently and share hundreds of millions of new posts, messages, photos, and videos every day. Facebook, for example, recently published a paper on its transition to a new file system for its data centers[14] in which each cluster "scales to exabytes," up from "tens of petabytes" in their previous system.

Each individual social media account for each user can easily contain hundreds or thousands of pages of materials in a mishmash of formats. For example, in the highly publicized case that led to the end of the US-EU Safe Harbor program, a law student requested all of Facebook's retained data on him[15] and received 1,222 pages that included: posts, messages, chat logs, log-on and posting times, records of his friends and connections, GPS data from photographs, some deleted materials, and more.

The student received those materials primarily in PDF format, but in their original formats, live on the Facebook platform, the files also would have carried their own metadata – both metadata typical of the file type and metadata specific to the social media platform. For example, files on Facebook may carry metadata fields documenting their unique identifier, item type, parent item, thread, recipients, author/poster, linked media, comments, and more. The other major platforms have comparable fields of their own in use.

RELIABILITY CONCERNS

In recent years, the Internet has seen a massive surge in deliberately fake content. Some of it is intended only to entertain[16] or advertise or get attention, but some of it is intended to sow confusion and misinformation.[17] While this may pose a challenge[18] to our discernment[19] of reliable public information, it remains generally unlikely that any individual – unless they are a public figure – would be impersonated online or have fake social media materials created in their name. There are valid questions, however, as to how reliable even "real" posts from users are. And, for individuals who are public figures, deepfakes have become a growing area of concern.

[12] *What categories of my Facebook data are available to me?, FACEBOOK HELP CENTER, https://www.facebook.com/help/405183566203254?helpref=faq_content (2021).*

[13] *Sean Gallagher, Facebook scraped call, text message data for years from Android phones, ARS TECHNICA, https://arstechnica.com/information-technology/2018/03/facebook-scraped-call-text-message-data-for-years-from-android-phones/ (Mar. 24, 2018).*

[14] *Consolidating Facebook storage infrastructure with Tectonic file system, FACEBOOK ENGINEERING, https://engineering.fb.com/2021/06/21/data-infrastructure/tectonic-file-system/ (June 21, 2021).*

[15] *Owen Bowcott, Facebook data privacy case to be heard before European Union court, THE GUARDIAN, https://www.theguardian.com/technology/2015/mar/24/facebook-data-privacy-european-union-court-maximillian-schrems (Mar. 24, 2015).*

[16] *Bill Bradly, Jimmy Kimmel Reveals He's Behind Another Popular Viral Video, THE HUFFINGTON POST, http://www.huffingtonpost.com/entry/jimmy-kimmel-reveals-another-of-your-favorite-viral-videos-is-fake_us_56246963e4b08589ef47e673 (Oct. 19, 2015).*

[17] *Craig Timberg, Russian propaganda effort helped spread 'fake news' during election, experts say, THE WASHINGTON POST, https://www.washingtonpost.com/business/economy/russian-propaganda-effort-helped-spread-fake-news-during-election-experts-say/2016/11/24/793903b6-8a40-4ca9-b712-716af66098fe_story.html (Nov. 24, 2016).*

[18] *Richard Gray, Lies, propaganda and fake news: A challenge for our age, BBC, http://www.bbc.com/future/story/20170301-lies-propaganda-and-fake-news-a-grand-challenge-of-our-age (Mar. 1, 2017).*

[19] *Belinda Luscombe, More Than Half of American Kids Say They Can't Spot Fake News, TIME, http://time.com/4694165/more-than-half-of-kids-say-they-cant-spot-fake-news/ (Mar. 8, 2017).*

Reliability of the Real

Just how reliable are individuals' own, real social media posts? Do people really create accurate, spontaneous reflections of themselves and their lives? Probably not, at least not entirely[20]:

> In a 2012 paper published in the Vanderbilt Journal of Entertainment & Technology Law, Kathryn R. Brown distilled recent research on social media psychology and found that users selectively screen photos to present themselves as "attractive" and "having fun," and that they tune their personae to come across as "socially desirable," "group-oriented," and "smiling." . . . Meanwhile, "individuals are unlikely to capture shameful, regrettable, or lonely moments with a camera."

So, to at least some extent, we all generate our own mildly "fake news" about ourselves, editing our comments and curating our images to try to appear as we wish to be seen rather than as we may be. This does not mean that there may not be reliable, valuable evidence to be had in social media materials but, rather, that we should consider such materials with this in mind and be conservative in the inferences we draw and the assumptions we make. As one judge put it[21]: "The fact that an individual may express some degree of joy, happiness, or sociability on certain occasions sheds little light on the issue of whether he or she is actually suffering emotional distress."

Deepfakes on the Horizon

Another source of potential complications in social media evidence is the rise of deepfakes. Deepfakes are "highly realistic, falsified imagery and sound recordings"[22] in which the original faces and/or voices are replaced with new ones. They are not created using the types of 3D rendering used for movie special effects but, rather, using publicly-available machine-learning algorithms trained using online source media (*i.e.*, images, videos, and audio recordings). They quickly progressed from illicit applications to viral social media amusements[23]:

> Like all video-adjacent technology, deepfakes first saw significant use in pornography, flooding the Internet with videos that to the untrained . . . eye look like celebrities doing porn. Otherwise, it's mostly used for comedy, like putting Steve Buscemi's face on Jennifer Lawrence, or swapping Arnold Schwarzenegger and Danny De Vito in Twins. Sometimes, deepfakers reinstate a role's "original" casting (like Tom Selleck as Indiana Jones), bring actors like Bruce Lee back from the dead, or – in this latest case – ponder remakes of classics with Marvel Cinematic Universe stars.

Deepfake technology has the potential to create a variety of serious legal complications, including discovery complications such as defendants challenging the authenticity of video or audio evidence against them (even when it's real) and a new potential need for video or audio analysis and expert testimony (and the costs that come with both).

[20] *Amanda Hess, Evidence of Life on Facebook, SLATE, https://slate.com/technology/2015/04/social-media-and-the-law-if-youre-claiming-emotional-distress-dont-appear-happy-on-facebook.html (Apr. 29, 2015); see also Kathryn R. Brown, The Risks of Taking Facebook at Face Value: Why the Psychology of Social Networking Should Influence the Evidentiary Relevance of Facebook Photographs, 14 VANDERBILT J. OF ENTM'T. AND TECH. L. 357 (2020), available at https://scholarship.law.vanderbilt.edu/jetlaw/vol14/iss2/3/.*

[21] *Giacchetto v. Patchogue-Medford Union Free Sch. Dist., 293 F.R.D. 112 (E.D.N.Y. 2013), available at https://casetext.com/case/theresa-giacchetto-plaintiff-v-patchogue-medford-union-free-school-district-defendants.*

[22] *Katherine B. Forrest, Deepfakes: When a Picture Is Worth Nothing at All, NEW YORK LAW JOURNAL, https://www.law.com/newyorklawjournal/2019/10/28/deepfakes-when-a-picture-is-worth-nothing-at-all/ (Oct. 28, 2019).*

[23] *Andrew Todd, Deepfakes: Visual Effects For The Post-Truth World, BIRTH. MOVIES. DEATH., https://birthmoviesdeath.com/2020/02/18/deepfakes-visual-effects-for-the-post-truth-world (Feb. 18, 2020).*

OBTAINING SOCIAL MEDIA EVIDENCE

Legal Mechanisms

While the publicly-shared materials on social media services can be collected directly by any party, the non-public materials in those user accounts can only be obtained through discovery. In general, social media materials are discoverable under the same conditions and in the same ways as any other type of evidence. As defined in Federal Rule of Civil Procedure 26(b),[24] the scope of permissible discovery is:

> Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case . . . . Information within this scope of discovery need not be admissible in evidence to be discoverable.

This standard applies to tweets, Facebook posts, or Instagram pictures the same way it does to more traditional sources like Office documents or emails. If it's relevant, it's discoverable, as recent state and federal court decisions have affirmed.[25] This may extend even to materials in which you are tagged, but which you did not post.[26]

Despite the discoverability standards being the same for social media sources as for other types of sources, parties have frequently ended up in disputes over the appropriate scope of discovery for these materials. Requesting parties have often made overbroad requests for all materials from a social media account, and producing parties have pushed back, asserting overbreadth, irrelevance, and privacy issues.[27]

Service Provider Subpoenas

Some litigants have attempted to obtain non-public social media materials by subpoenaing those materials directly from the social media service providers. Unfortunately for the requesting parties, those attempts have run up against Title II of the Electronic Communications Privacy Act of 1986,[28] which is also known as the Stored Communications Act (SCA). The SCA establishes certain privacy protections for our electronic materials stored with third party service providers, from both government intrusion and third party access.

In the case of *Crispin v. Christian Audigier, Inc.*,[29] a party issued subpoenas to Facebook and Myspace seeking specified, non-public materials from the opposing party's accounts. A Federal District Court judge later quashed those subpoenas, finding that Facebook and Myspace qualified as "electronic communication services" under the SCA, which therefore prohibited the desired disclosures. More recently, in the case of *Ehling v. Monmouth-Ocean Hospital Service Corp.*[30] a Federal District Court Judge again determined non-public Facebook materials to be protected by the SCA (in a non-discovery context).

In a May 2018 decision discussing service provider subpoenas in the criminal context,[31] the California Supreme Court held that service providers must comply

[24] *Fed. R. Civ. P.26(b), available at https://www.law.cornell.edu/rules/frcp/rule_26.*

[25] *See e.g. Forman v. Henkin, 30 N.Y.3d 656 (N.Y. Feb 13, 2018) (rejecting "heightened threshold" for discovery of these materials and finding privacy settings no bar), available athttps://law.justia.com/cases/new-york/court-of-appeals/2018/1.html, and Michael Brown, Sr. v. City of Ferguson, 2017 WL 386544 (E.D. Mo. Jan. 27, 2017) (finding privacy no bar to discovery of these materials when relevant), available at https://www.leagle.com/decision/infdco20170130926.*

[26] *See e.g. Vasquez-Santos v. Mathew, 168 A.D.3d 587 (App. Div. 1st Dep't Jan. 24, 2019), available at http://nycourts.gov/reporter/3dseries/2019/2019_00541.htm.*

[27] *See e.g. Ehrenberg v. State Farm Mut. Auto. Ins. Co., No. 16-17269 (E.D. La. Aug. 18, 2017) (ordering production of social media materials, but limiting to relevant scope), available at https://www.govinfo.gov/content/pkg/USCOURTS-laed-2_16-cv-17269/pdf/USCOURTS-laed-2_16-cv-17269-0.pdf; Madeline Scott v. United States Postal Service, et al., 2016 WL 7440468 (M.D. La. Dec. 27, 2016) (ordering production of social media materials materials, but limiting to relevant scope), available at https://scholar.google.com/scholar_case?case=2652101794339924070; and, Locke v. Swift Transp. Co. of Arizona, LLC, et al., 2019 WL 430930 (W.D. Ky. Feb. 4, 2019) (ordering production of social media materials, but limiting to relevant scope), available at https://law.justia.com/cases/federal/district-courts/kentucky/kywdce/5:2018cv00119/108084/32/.*

[28] *Electronic Communications Privacy Act of 1986, Pub. L. 99-508 (Oct. 21, 1986), available at https://www.justice.gov/sites/default/files/jmd/legacy/2013/09/06/act-pl99-508.pdf.*

[29] *Crispin v. Christian Audigier, Inc., 717 F.Supp.2d 965 (C.D. Cal. 2010), available at https://www.leagle.com/decision/inadvfdco110214000105.*

[30] *Ehling v. Monmouth-Ocean Hospital Service Corp., 961 F.Supp.2d 659 (D.N.J. Aug. 20, 2013), available at https://www.insideprivacy.com/wp-content/uploads/sites/6/2013/09/Ehling-v.-Monmouth-Ocean-Hospital-SCA.pdf.*

[31] *Facebook, Inc. v. Superior Court, 4 Cal.5th 1245 (Cal. May 24, 2018), available at https://law.justia.com/cases/california/supreme-court/2018/s230051.html.*

with subpoenas from criminal defendants for public materials, but it did not resolve the larger question of when criminal defendants' rights under the Fifth and Sixth Amendments might trump the SCA[32] and entitle them to obtain private social media materials via service provider subpoena. More recently, in the District of Columbia case of *Facebook, Inc. v. Wint*,[33] the appellate court reaffirmed the general rule that the SCA prevents criminal defendants (and civil litigants) from obtaining covered communications from service providers using subpoenas (absent one of the statute's explicit exceptions).

The updated Sedona Conference Primer[34] suggests the use of preservation subpoenas to service providers as an alternative. Subpoenas seeking preservation rather than production would not run afoul of the SCA's restrictions on service provider production, but should help ensure materials remain available while other approaches to obtaining discovery of them are pursued.

Collection Process

There are three main approaches to the collection of social media materials for use in litigation:

1. The most basic is printing out the material or capturing a screen image of it. This has the advantages of being fast, simple, and cheap, but it comes with significant drawbacks. First, you will not have captured the native file or any associated metadata, and second, unless the other party concedes the authenticity and accuracy of the print or image copy, you may have a hard time getting such a copy authenticated and admitted as evidence. This approach may be sufficient for an internal investigation, but it is not generally sufficient for litigation.[35]

2. One level up from printing or screen capturing content is using the self-service export tools provided by the social media platform instead. Many social media platforms, including Facebook[36] and Twitter,[37] offer a mechanism for a user to download materials associated with their account. These kinds of features export a package of a user's materials, which may be in a mixture of files and formats or may just be combined in a single PDF, depending on the platform and the materials in the account. This, too, is fast and cheap, but it may not be simple or sufficient: first, it can only be done by the account holder (or by someone with their credentials and consent); second, the length and format can make the export challenging to sort through and separate once obtained; and, third, the export may not provide native files with metadata (creating authentication issues), and it won't have any of the linked content embedded from other sites.

3. An additional level up from the use of self-service export tools is the use of specialized forensic collection software. Such tools capture the files and materials, along with their metadata and any linked content, and provide options for searching, sorting, and filtering. Depending on the tool and the target source, they may accomplish this through API access, dynamic capture, web archiving, or some combination of these approaches. Using a tool like this carries additional costs, but it can be essential for cases involving large quantities of social media materials, questions best resolved through metadata, or the potential for disputes over the authenticity and admissibility of the materials.

[32] *Stephanie Lacambra, A Constitutional Conundrum That's Not Going Away—Unequal Access to Social Media Posts, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/deeplinks/2018/05/ca-supreme-court-leaves-scales-tipped-prosecutions-favor-defense-gets-access (May 31, 2018).*

[33] *Facebook, Inc. v. Wint, 199 A.3d 625 (D.C. App. Jan. 3, 2019), available at https://www.dccourts.gov/sites/default/files/2019-01/18-CO-958.pdf.*

[34] *The Sedona Conference, supra.*

[35] *See e.g. Cordova v. Walmart Puerto Rico, Inc. et al., 2019 WL 3226893 (D.P.R. 2019), available at https://casetext.com/case/cordova-v-walmart-pr-inc, and Edwards, Jr. v. Junior State of Am. Found., 2021 WL 160028 (E.D. Tex. 2021), available at https://law.justia.com/cases/federal/district-courts/texas/txedce/4:2019cv00140/188037/129/.*

[36] *Alexia Tsotsis, Facebook Now Allows You To "Download Your Information," TECHCRUNCH, https://techcrunch.com/2010/10/06/facebook-now-allows-you-to-download-your-information/ (Oct. 6, 2010).*

[37] *Mollie Vandor Forer, Your Twitter archive, TWITTER BLOG, https://blog.twitter.com/2012/your-twitter-archive (Dec. 10, 2012).*

AUTHENTICATION

In order for any of the materials you have collected to be usable at trial, they will have to be successfully admitted as evidence. The admissibility of a particular piece of evidence turns on a variety of factors, but the most foundational requirement evidence must satisfy is that it must be authentic, *i.e.* it must actually be whatever it purports to be. This is essential for the obvious reason that fake or falsified materials cannot carry any weight as evidence.

Unfortunately, in the context of social media evidence, the question of authenticity can be a challenging one. Social media platforms are still relatively new, legally speaking, and they are constantly evolving in form and content. Moreover, many individuals still view all Internet sources as inherently suspect. The following passage about "voodoo information taken from the Internet" is from *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, [38] which predates the social media boom but illustrates well the suspicion some feel towards Internet sources:

> While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity . . . . There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy.
>
> Anyone can put anything on the Internet. No web-site is monitored for accuracy and nothing contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on any web-site from any location at any time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation . . . .

As a result, there has been a great deal of disagreement about when and how social media materials should be authenticated and admitted.

Authenticity and the Federal Rules

The process for establishing evidentiary authenticity is laid out in Federal Rule of Evidence 901.[39] To establish authenticity, "the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." The rule goes on in subpart (b) to provide a non-exclusive list of ten example ways that authenticity might be shown for various types of evidence. Among them are two example methods of particular relevance to the authentication of social media materials:

- **901(b)(1) "Testimony of a Witness with Knowledge"**
  - A witness with knowledge can provide authenticating testimony. For social media materials, that might be testimony from the person who created the materials or a person who received the materials. Unfortunately, authenticating testimony from the creator or author may not be available when the material is unfavorable evidence for that individual. For that reason, distinctive characteristics are very important.
- **901(b)(4) "Distinctive Characteristics and the Like"**

[38] *St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F.Supp.2d 773 (1999), available at http://www.leagle.com/decision/199984976FSupp2d773_1764/ST. CLAIR v. JOHNNY'S OYSTER & SHRIMP, INC..*

[39] *Fed. R. Evid. 901, available at https://www.law.cornell.edu/rules/fre/rule_901.*

- Distinctive characteristics of a piece of evidence can be considered to establish its authenticity. Distinctive characteristics are specific details of the material that make it likely the material is authentic. For social media materials, distinctive characteristics might include (but are not limited to): materials appearing on a page that is in the alleged author's name; relevant individuals appearing in included pictures; relevant topics being discussed; distinctive slang being used; the appearance of relevant names or nicknames; the times or locations on shared posts or photos; or, the IP address of the device from which posts were made. In other words: "If it looks like a duck, waddles like a duck, and quacks like a duck, it must be a duck."[40]

Even if a showing sufficient to establish authenticity is made, however, the authenticity of the evidence can still be challenged by a similar, contrary showing from another party. In the event of conflicting showings regarding the authenticity of some piece of evidence, what arises is a situation where relevance depends on a factual determination: if the underlying facts about the offered evidence are as the submitting party contends, the evidence is authentic and relevant; if instead the underlying facts about the offered evidence are as the opposing party contends, the evidence is inauthentic and, therefore, irrelevant.

Such situations are governed by Federal Rule of Evidence 104(b)[41] "Relevance That Depends on a Fact," which requires that "proof must be introduced sufficient to support a finding that the fact does exist." As long as that required proof is offered, the original social media evidence and the proof supporting its authenticity can be put to the jury for a factual determination regarding authenticity, which will in turn determine relevance, as is done with other evidence types:

> . . . courts historically considered admissibility of all documentary evidence on a continuum, in which clearly authentic evidence is admitted, clearly inauthentic evidence is excluded, and everything in between is conditionally relevant and admitted for the jury to determine its authenticity.[42]

This is how the application of the rules to social media materials should work, but in practice, that has not always been the case. Some courts have instead held social media materials to a higher stand for authentication because of fears that it may just be "voodoo information."

Authentication in the Courts: A Tale of Two States

The story of social media authentication in the courts is a tale of two states: Maryland and Texas. These were two of the first states to address these issues at the appellate level, and each staked out a different position: the Maryland case expressed inherent mistrust of social media and set a higher bar for such evidence to reach the jury, while the Texas case tracked the intended operation of the evidentiary rules above, treating social media evidence like other types of evidence. Both states' approaches have since been followed by other states, but the Texas approach has been much more-widely adopted[43] than the Maryland approach.[44]

[40] *Paul W. Grimm, Lisa Yurwit Bergstrom & Melissa M. O'Toole-Loureiro, Authentication of Social Media Evidence, 36 Am. J. Trial Advoc. 433 (2013), available at http://www.atyvideo.com/documents/American Journal of Trial Advocacy Authentication of Social Media Evidence.pdf.*

[41] *Fed. R. Evid. 104(b), available at https://www.law.cornell.edu/rules/fre/rule_104.*

[42] *Grimm, supra.*

[43] *See e.g. Burgess v. State, 742 S.E.2d 464 (Ga. 2013), available at https://casetext.com/case/burgess-v-state-225; Parker v. State, 85 A.3d 682 (Del. 2014), available at https://www.leagle.com/decision/indeco20140206069; State v. Jones, 318 P.3d 1020 (Kan. App. 2014), available at https://casetext.com/case/state-v-jones-4057; State v. Snow, 437 S.W.3d 396 (Mo. Ct. App. S.D. 2014), available at https://casetext.com/case/state-v-snow-78; State v. Gibson, 2015 WL 1962850 (Ohio App. 6 Dist. 2015), available at http://www.supremecourt.ohio.gov/rod/docs/pdf/6/2015/2015-Ohio-1679.pdf; and, State v. Burns, 2015 WL 2105543 (Tenn. Crim. App. 2015), available at https://cases.justia.com/tennessee/court-of-criminal-appeals/2015-m2014-00357-cca-r3-cd.pdf.*

[44] *See e.g. Smith v. State, 136 So.3d 424 (Miss. 2014), available at https://casetext.com/case/smith-v-state-7769; People v. Glover, 363 P.3d 736 (Colo. App. 2015), available at https://www.leagle.com/decision/incoco20150226102; and, Commonwealth v. Mangel, 2018 PA Super 57 (Pa. Super. Ct. 2018), available at https://www.leagle.com/decision/inpaco20180315753.*

Griffin and the Maryland Approach

The case of *Griffin v. State of Maryland*[45] was a criminal case in which the prosecution introduced printouts of the relevant social media messages and profiles into evidence. They attempted to authenticate the social media materials using Maryland's equivalent of FRE 901(b)(4) and the distinctive characteristics of the materials. The distinctive characteristics they identified for the court included matching the profile's displayed age, city, birthday, photograph, children, and nickname use with those of the alleged owner of the profile and author of the posts. The trial court judge allowed the admission of the evidence, with instructions to the jury about how to evaluate what weight to give it.

The admission of the materials was upheld on its appeal to Maryland's Court of Special Appeals but reversed on its subsequent appeal to the Maryland Court of Appeals. In reaching its decision, that court expressed inherent mistrust of social media sources:

> The potential for abuse and manipulation of a social networking site by someone other than its purported creator and/or user leads to our conclusion that a printout of an image from such a site requires a greater degree of authentication than merely identifying the date of birth of the creator and her visage in a photograph on the site in order to reflect that [she] was its creator and the author . . . .

The court suggested that it might have accepted the materials as authentic if the prosecution had gone beyond distinctive characteristics and had, for example: gotten the author to testify to her authorship, gotten forensic evidence from the device used for the post, or gotten IP address evidence from the social media service.

Later, in *Sublet v. State*[46] the court clarified its *Griffin* ruling as having been a nonexclusive list of authentication examples, and it nominally adopted the standard as articulated by the Second Circuit in *United States v. Vayner*,[47] which is consistent with the Federal rules approach discussed above. Some took this to mean the court had moderated its position, but in the decision, the court also reaffirmed its conclusion in *Griffin* and continued to express inherent mistrust of internet sources at the mercy of fakery or alteration by "crackers," creating ambiguity. Five years later, in *State v. Sample*,[48] the court again revisited the issue, and applied the Second Circuit standard without the reservations previously expressed in *Sublet*.

Tienda and the Texas Rule

The case of *Tienda v. State of Texas*[49] was also a criminal case in which the prosecution introduced into evidence printouts of three MySpace profiles and related content alleged to be the defendant's. The prosecution used the materials, "Subscriber Reports" from the social media service, and testimony from someone with knowledge to highlight distinctive characteristics of the materials including: names and nicknames, locations, people appearing in photos, messages and posts referencing relevant events and details.

The trial judge admitted the materials for the jury to consider, over the objections of the defendant, and that decision was affirmed on appeal to the Texas Fifth Court of Appeals. The defendant appealed again to the Texas Court of Criminal Appeals, but that court too affirmed the admission of the materials based on the *prima facie* showing of authenticity that had been made using distinctive characteristics: "This combination of facts . . . is

[45] *Griffin v. State of Maryland, 419 Md. 343 (Md. 2011), available at https://www.courts.state.md.us/data/opinions/coa/2011/74a10.pdf..*

[46] *Sublet v. State, 442 Md. 632 (Md. 2015), available at https://casetext.com/case/sublet-v-state-5.*

[47] *United States v. Vayner, 769 F.3d 125 (2d Cir. 2014), available at https://casetext.com/case/united-states-v-vayner-1.*

[48] *State v. Sample, 468 Md. 560 (Md. 2020), available at https://casetext.com/case/state-v-sample-25.*

[49] *Tienda v. State of Texas, 358 S.W.3d 633 (Tex. Crim. App. 2012), available at https://casetext.com/case/tienda-v-state-10.*

sufficient to support a finding by a rational jury that the MySpace pages that the State offered into evidence were created by the appellant."

The court also addressed directly the "voodoo information" concerns and how the rules already address them without the need for a special, higher bar:

> It is, of course, within the realm of possibility that the appellant was the victim of some elaborate and ongoing conspiracy. Conceivably some unknown malefactors somehow stole the appellant's numerous self-portrait photographs, concocted boastful messages . . . . But that is an alternate scenario whose likelihood and weight the jury was entitled to assess once the State had produced a *prima facie* showing that it was the appellant, not some unidentified conspirators or fraud artists, who created and maintained these MySpace pages.

SPOLIATION

Social media materials are being implicated more and more frequently, making their preservation and spoliation real concerns. The cases discussing social media spoliation issues make clear that, while parties and their attorneys may still be struggling with social media, courts are very comfortable treating it like any other source: if relevant, it needs to be preserved and produced; and, under no circumstances, should it be intentionally altered, deleted, or hidden.

Changing Relevant Social Media – *Katiroll* (2011)

In the case of *The Katiroll Company, Inc. v. Kati Roll and Platters, Inc.*,[50] the defendant changed their Facebook profile picture from one that included the dress the trademark dispute was over to one that did not. The plaintiff sought spoliation sanctions over that change, but the court found that changing social media profile pictures is common and that the spoliation was probably unintentional. To address the minor prejudice it caused, the court directed the prior profile picture temporarily restored and a screen capture made for use as evidence.

Deliberate Spoliation – *Allied Concrete* (2013)

In the case of *Allied Concrete Co. v. Lester*,[51] an attorney advised a client to "clean up" his Facebook page and suggested some images that should be removed. The client ultimately deleted 16 pictures and then, later, deleted the whole account and claimed not to have one. The deletions were established[52] using IP logs obtained from Facebook and expert testimony. Ultimately, the misconduct resulted in an adverse inference instruction to the jury, a $722,000 award of costs and fees against the client and the attorney, and a five-year suspension for the attorney.[53]

[50] *The Katiroll Company, Inc. v. Kati Roll and Platters Inc., 2011 WL 3583408 (D.N.J. 2011), available at http://law.justia.com/cases/federal/district-courts/new-jersey/njdce/3:2010cv03620/244223/255/.*

[51] *Allied Concrete Co. v. Lester, 285 Va. 295 (Va. 2013), available at https://scholar.google.com/scholar_case?case=12929440551591006221.*

[52] *K&L Gates, Client & Counsel Sanctioned for Spoliation Where Plaintiff Was Instructed to "Clean Up" His Facebook Page, ELECTRONIC DISCOVERY LAW, https://www.ediscoverylaw.com/2011/11/client-counsel-sanctioned-for-spoliation-where-plaintiff-was-instructed-to-clean-up-his-facebook-page/ (Nov. 18, 2011).*

[53] *Debra Cassens Weiss, Lawyer agrees to five-year suspension for advising client to clean up his Facebook photos, ABA JOURNAL, http://www.abajournal.com/news/article/lawyer_agrees_to_five-year_suspension_for_advising_client_to_clean_up_his_f (Aug. 7, 2013).*

Accidental Deletion – *Gatto* (2013)

In the case of *Gatto v. United Airlines, Inc.*,[54] the plaintiff produced his Facebook password to the defendants so they could access, review, and print some agreed-upon materials. When they attempted to access the account, however, the plaintiff received an automatic notification from Facebook about an access attempt from a new, unauthorized IP address and – allegedly fearing hacking – deactivated his account. He later attempted to restore it, but after two weeks of deactivation, Facebook had already deleted the account materials (per its standard policy) making them unrecoverable. Based on the loss of those materials and the prejudice it caused to the defendants, the court granted an adverse inference instruction regarding the spoliated Facebook evidence.

Failure to Preserve – *Painter* (2014)

In the case of *Painter v. Atwood*,[55] the defendants sought spoliation sanctions over the deletion of Facebook posts by the plaintiff that, allegedly, would have contradicted or undermined her claims in the case. Plaintiff's attorney conceded that the deletion had occurred but argued that the posts were irrelevant and that "[p]laintiff is a 22-year old girl who would not have known better than to delete her Facebook comments." The court rejected both arguments:

> First, Plaintiff's Facebook comments discussing her opinion on working and interacting with Defendant . . . are directly relevant to this litigation. . . . Second . . . it is of no consequence that Plaintiff is young or that she is female and, therefore, according to her counsel, would not have known better than to delete her Facebook comments. Once Plaintiff retained counsel, her counsel should have informed her of her duty to preserve evidence and, further, explained to Plaintiff the full extent of that obligation.

The court went on to determine that an adverse inference sanction would be the appropriate remedy for the loss of the Facebook materials.

Deactivation Deception – *Crowe* (2015)

In the case of *Crowe v. Marquette Transp. Co. Gulf-Inland, LLC*,[56] the plaintiff deactivated his Facebook account days after receiving a discovery request to produce materials from it, and then, he claimed he did not "presently have a Facebook account." Since the account had been deactivated rather than deleted, materials could still be recovered, however, and the court ordered the production of all materials, the turning over of account credentials, and consent/cooperation for any subpoenas the defendant wished to issue directly to Facebook.

Changing Accessibility – *Thurmond* (2016)

In the case of *Thurmond v. Bowman*,[57] the defendants sought spoliation sanctions against the plaintiff over the disappearance of numerous allegedly-relevant posts from her Facebook account. Ultimately, it was determined that the plaintiff had made a privacy settings change to the account that changed the public visibility of the posts but had not deleted them. The plaintiff produced the materials, and the court declined to apply sanctions, but the court did express its displeasure with the plaintiff's "troubling" conduct and indicated that sanctions might be applied for further inappropriate conduct.

[54] *Gatto v. United Airlines, Inc., et al., 2013 WL 1285285 (D.N.J. 2013), available at https://docs.justia.com/cases/federal/district-courts/new-jersey/njdce/2:2010cv01090/238467/42/.*

[55] *Painter v. Atwood, 2014 WL 1089694 (D. Nev. 2014), available at https://cases.justia.com/federal/district-courts/nevada/nvdce/2:2012cv01215/88734/75/0.pdf.*

[56] *Crowe v. Marquette Transp. Co. Gulf-Inland, LLC, 2015 WL 254633 (E.D. La. Jan. 20, 2015), available at https://docs.justia.com/cases/federal/district-courts/louisiana/laedce/2:2014cv01130/161984/32.*

[57] *Thurmond v. Bowman, 2016 WL 1295957 (W.D.N.Y. 2016), available at https://www.theemployerhandbook.com/files/2016/05/Thurmond-v-Bowman-1.pdf.*

Hidden Account and Native File Deletion – *Cordova* (2019)

In the case of *Cordova v. Walmart Puerto Rico*,[58] the defendants sought production of relevant social media materials from the plaintiff. Initially, the plaintiff "responded, in essence, that she once had a social media account, but that it was closed and that she did not recall the name under which she had the account." The plaintiff's story evolved several times, however, after the defendants were "able to identify plaintiff's public Facebook profile under the name '*Córdova Eigna*' – essentially, plaintiff's second last-name and her first name spelled backwards."

The plaintiff then produced printouts of some of her Facebook profile and some related photographs. The defendants noted that needed metadata and other materials were not included and sought supplementation in native format, but the plaintiff "responded that she had deleted her Facebook account after her previous production." The defendants sought dismissal as a sanction, arguing that the overall course of conduct and the ultimate spoliation amounted to "fraud on the Court."

The court held that the plaintiff had "failed to comply with her obligation under Fed. R. Civ. 26(e) to supplement discovery responses" and that the plaintiff's "deletion of her Facebook account amounts to spoliation," which "may have caused prejudice" by depriving the defendants of "relevant metadata that would have been contained in the deleted Facebook page." The court did not find, however, that the plaintiff had committed fraud on the court and, so, applied an adverse-inference jury instruction sanction rather than dismissal.

Screenshots No Substitute for Deleted Native Files – *Edwards* (2021)

In the case of *Edwards, Jr. v. Junior State of America Foundation*,[59] the defendant sought production of "ESI from [the plaintiff's] Facebook Messenger account that could prove or refute the authenticity of the alleged Messages" that were central to the case. They also provided an explanation of "how to produce messages in HTML format." The plaintiff, however, "never objected or responded to any of the Requests for Production that were served upon him."

This pattern of pursuit and avoidance continued for approximately the next nine months, after which the defendant filed a motion to compel production of the ESI, along with a motion for sanctions "for failure to comply with discovery requests." The plaintiff did not respond to either motion, and after a hearing, the court granted both.

Subsequently, the plaintiff produced two expert affidavits and a forensic report, but this production still did not include "the native Facebook-message files, *i.e.*, proof of the alleged Messages in JSON or HTML format, as requested . . . and as required by Court order." The defendant then filed a "Motion to Dismiss Pursuant to Rule 37 for Failing to Comply with a Court Order to Produce Electronically Stored Information." In the plaintiff's response to this motion, he explained that he "cannot produce the native-file Messages because they have been permanently deleted."

The court analyzed the plaintiff's assorted discovery misconduct under FRCP 37(b), (c), and (e)(1),[60] focusing on the screenshots-versus-native-files issue as part of its spoliation analysis under (e)(1). The court found it indisputable that the plaintiff had been obligated to preserve the native files rather than just the partial screenshots:

[58] *Cordova v. Walmart Puerto Rico, Inc. et al., 2019 WL 3226893 (D.P.R. 2019), available at https://casetext.com/case/cordova-v-walmart-pr-inc.*

[59] *Edwards, Jr. v. Junior State of Am. Found., 2021 WL 160028 (E.D. Tex. 2021), available at https://law.justia.com/cases/federal/district-courts/texas/txedce/4:2019cv00140/188037/129/.*

[60] *Fed. R. Civ. P. 37, available at https://www.law.cornell.edu/rules/frcp/rule_37.*

Further, Plaintiffs cannot persuasively contend that they did not know or should not have known of their **need to preserve the actual Messages as opposed to screenshots** thereof. . . . Pursuant to Federal Rule of Evidence ("FRE") 1002, the so-called "Best Evidence Rule" provides that "[a]n original writing, recording, or photograph is required to prove its contents unless these rules or a federal statute provide otherwise." As it is applied to ESI, FRE 1001(d) provides that "original" "means any printout – or other output readable by sight – if it accurately reflects the information." **Here, the screenshots will not suffice as an "original" because the screenshots are not an "output" that "accurately" reflect the information. Only native files can ensure authenticity**. Additionally, although the Best Evidence Rule allows for an original "photograph" to prove the contents of the photograph, this does not mean that the screenshot here can be used to prove that [the alleged author] sent the Facebook Messages contained in the screenshots. Instead, **the screenshots prove only that [the plaintiff took a screenshot containing what appears to be Facebook Messages – not that the Messages are authentic or that [the alleged author] indeed sent the Messages**. Second, however, one need not be familiar with the Best Evidence Rule to understand that the actual Messages may be important in proving that someone sent the Messages in question and that screenshots may be insufficient to that end. **That the actual Messages may be relevant to the instant litigation is self-evident. Accordingly, the [plaintiff] had a duty to preserve the native files, *i.e.*, the actual alleged Facebook Messages, because plaintiffs had either actual or constructive notice as to the files' relevance.** [emphasis added]

Ultimately, after finding all the elements of FRCP 37(e)(1) satisfied, the court entered an order excluding "all evidence and testimony of the purported text exchange" and prohibiting the plaintiff "from offering any evidence of the alleged Messages."

Key Takeaways

There are seven key takeaways from this white paper to remember:

1. Social media is used frequently by the majority of people in the United States, and it is showing up in more cases as evidence each year. Currently, the most commonly used social media platforms are YouTube, Facebook, Instagram, Pinterest, LinkedIn, Snapchat, and Twitter. Facebook is the source that has, so far, shown up most often in cases. New services continue to arise, however, (e.g., TikTok) and usage patterns continue to evolve.

2. Collectively, social media users generate enormous numbers of posts, messages, photos, videos, and other content each day, and each individual account can contain large quantities of material, in many formats, including both native and platform metadata. Additionally, service providers typically keep IP logs and other records.

3. Truly fabricated materials are not a likely issue, unless your client is a public figure (in which case impersonation or deepfakes may become an issue), but individuals' tendency to portray themselves in the best light possible makes the materials' utility for discerning mental or emotional states questionable. Take them with a grain of salt.

4. Social media evidence is discoverable, like all evidence, when it is relevant. Overbroad requests are disfavored and likely to be limited by the judge. Because of the Stored Communications Act, subpoenas to obtain materials directly from the social media service providers are unlikely to work, but preservation subpoenas may be an option to buy time.

5. Self-help collection options are extremely limited, but they are okay in some situations (e.g., internal investigations, cases where authenticity is conceded). Forensic tools and services are available for when more complete collection or more robust post-collection options are needed.

6. Like all evidence, social media evidence must be authentic to be relevant and admitted. Social media is most often authenticated through the testimony of someone with knowledge and through the distinctive characteristics of the materials offered. When authenticity is disputed, most jurisdictions follow the Texas approach, which just requires the usual showing to reach the jury, while a few follow the Maryland approach, which requires a special, higher showing for social media evidence to reach the jury.

7. Attorneys and their clients may still be struggling to treat social media like other source types, but judges are not. If it's relevant, it needs to be preserved, and clients need to be advised of that fact explicitly. If it's lost, even unintentionally, curative measures and sanctions may follow.

ABOUT THE AUTHOR

Matthew Verga is an attorney, consultant, and eDiscovery expert proficient at leveraging his legal experience, his technical knowledge, and his communication skills to make complex eDiscovery topics accessible to diverse audiences. A fourteen-year industry veteran, Matthew has worked across every phase of the EDRM and at every level, from the project trenches to enterprise program design. As Director of Education for Consilio, he leverages this background to produce engaging educational content to empower practitioners at all levels with knowledge they can use to improve their projects, their careers, and their organizations.

Matthew Verga, Esq.
Director of Education
m +1.704.582.2192
e matthew.verga@consilio.com
consilio.com