Best Practices for Searching Social Media for Evidence

"While it's sometimes easy to find a person's social media page by their name, finding a page which a user has created under a different name or alias - making sure you have the correct page as well as assuring that you have captured all the data in accordance with the best practices can be a challenging task."

The approach involves a two step process of first conducting the searches and second preserving the evidence using a forensic approach that captures all the data. The purpose of this article is to provide a consistent, comprehensive approach for searching the internet while following the best practices and ethical standards.

"Social media evidence can have a direct impact on the outcome of a case"

Internet and social media evidence is not only useful in family and criminal litigation, but can influence personal injury, workers' compensation, product liability, and commercial litigation and employment cases.

This information can be used to establish an alibi, to assess the credibility of a witness, gain intelligence and background, identify and locate witnesses and be used to check the background and monitor the activities of jurors.

INDUSTRY STANDARDS

Attorneys are expected to be versed in digital evidence and be able to utilize technology, including social media, to provide competent and diligent representation.

Researching the online publicly available presence of potential parties, witnesses, the scene, even your own client should be a routine practice. It should follow the best practices, begin as soon as possible, be fully documented and be regularly monitored.

The key is to make sure that you're accessing the information in a permissible and ethical manner. It is inappropriate to bypass privacy settings to attempt to gain access to private pages that are not publicly available.

Equally important is understanding that internet and social media evidence is fleeting and time sensitive so beginning the searches should start as soon as possible.

A defined set of best practices and industry standards exist governing the preservation and analysis of internet and social media evidence.

The U.S Department of Justice - National Institute of Justice (NIJ) has published a comprehensive Special Report titled Investigations Involving the Internet and Computer Networks.

The Industry Standards/Best Practices and other informational materials are
available on our website in our Digital Evidence Toolbox
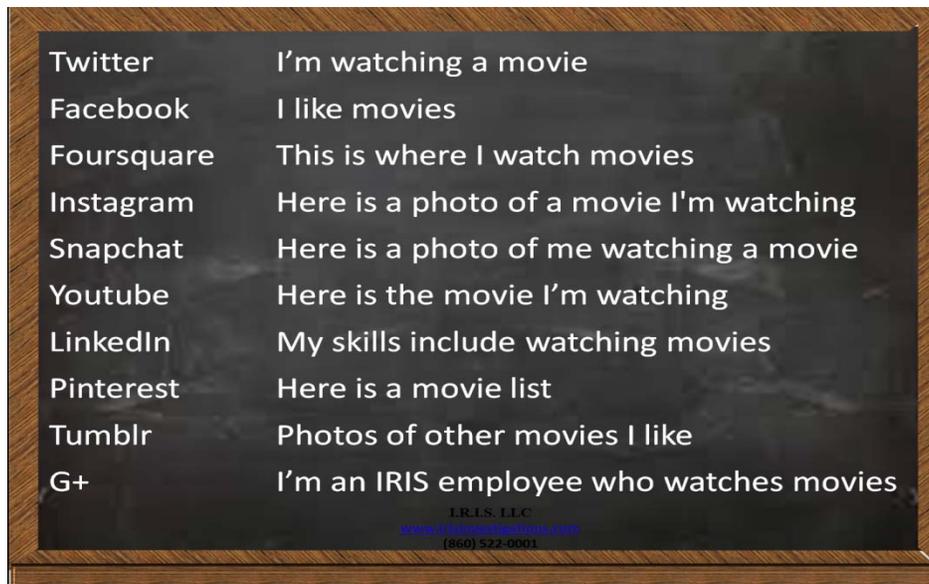
TYPES OF EVIDENCE

"In 2017, eighty-one percent of Americans had a social media profile."

Some examples of these sites include:

- Social networks such as Facebook and LinkedIn
- Web sites
- Blog sites such as Twitter and WordPress
- File sharing sites such as YouTube, Pinterest, Tumblr, Instagram and Flickr
- Activity and review sites such as Foursquare and Yelp
- Web based e-mail such as AOL, Gmail, Yahoo Mail

SOCIAL MEDIA EXPLAINED

Twitter	I'm watching a movie
Facebook	I like movies
Foursquare	This is where I watch movies
Instagram	Here is a photo of a movie I'm watching
Snapchat	Here is a photo of me watching a movie
Youtube	Here is the movie I'm watching
LinkedIn	My skills include watching movies
Pinterest	Here is a movie list
Tumblr	Photos of other movies I like
G+	I'm an IRIS employee who watches movies

I.R.I.S. LLC
www.irisinvestigations.com
(860) 522-0001

Twitter

- Basically a blogging platform with a 280 character limit

Facebook

- Content, images and videos
- Publicly announce plans
- Join groups
- Like topics
- Exchange private messages

Four Square

- Uses device's location services: GPS signal, Cell tower triangulation, Cellular signal strength, Surrounding Wi-Fi signals
- Digitally interact with the physical world
- Historical data
- User's name
- Profile photo
- Home city
- User biography
- Links to connected Twitter & Facebook accounts
- Check-ins shared to Twitter & Facebook
- Tips & lists
- Check-in comments
- Here now facepile
- Public check-in photos

Instagram

- Capture, edit and share photos, videos and messages

Snapchat

- Mobile only app
- Securely share messages, photos, and videos
- Destroyed after 24-hours
- Contact list (phone numbers)
- Precise location
- Text messages
- Phone status/identity
- Contents of the phone's USB storage

Pinterest

- Upload, save, sort, and manage content from around the web which user aspires to do in the future.
- Connects with Facebook, Twitter, Google+Gmail

Tumblr

- Post multimedia and other content to a short-form blog
- Users can follow other users' blogs
- Shows user's interests and lifestyle

"There can be no reasonable expected right to privacy in a tweet sent around the world"

-People v. Harris 2012

Privacy Considerations

Social media sites provide the user with privacy options and can be set so that some of the material is only available to some users while other information may be accessible to the general public.

If information can be accessed through public means without deceptively requesting the information from the individual or one of the individual's friends, it is "fair use."

Acquiring private data in violation of lawyer ethics rules could make the evidence inadmissible. It often is a violation of the Electronic Communications Privacy Act and other laws.

"Contacting witnesses via social media should follow the same rules as direct witness contact"

Examples of Unethical Practices

1. Pre-texting: Using a false identity to "friend" a person to gain access to their private information. In some cases, this can lead to criminal charges.

2. Contact with a represented party: Sending a friend request to a represented party in a pending action would violate ethical rules for communicating with the represented party about the pending action.

3. Reasonable Expectation of Privacy: If an employee of a company posts on a company social networking site using company equipment, there may be no expectation of privacy. However, it becomes less clear if company equipment is used to post on a personal account, and may depend on whether the company has an Acceptable Use Policy signed by the employee.

4. Spoliation: Directing a client to clean up or take down an account may be considered efforts to conceal or destroy evidence.

Note: There is a difference of opinion about whether a friend request from a lawyer or lawyer's agents that uses real names but does not disclose its litigation related purpose is ethical.

SEARCHING

Getting Started

Every situation should be assessed early on for possible sources of social media and internet evidence by the involved parties, first degree associates, witnesses and the scene itself. The searches will be conducted simultaneously on open source engines like Google, Yahoo and Bing as well as specific social media platforms.

The search criteria will differ, but the more that is known about the target the more searches that can be run. For example an email address of a witness would be good criteria to search for in an effort to identify a screen name that could lead to the discovery of social media sites.

Setting Up User Accounts for Searching

User profile accounts need to be created for each platform to be searched. The profile account should comply with the site's terms of service and in accordance with your company or agency's policies. The privacy settings should be enabled and the profile should have no friends or followers.

Because each platform has their own user and privacy terms of service, there is a difference of opinion as to what type, or ethically, what information should be contained in a profile account used to do social media searches.

Creating an account profile under a fake name could be in violation of the site's terms of service. Using that fake account to make contact with witnesses could be considered unethical because the witness could claim there were misled.

For mobile only apps such as Snapchat the search will have to be done either on a mobile device or through the use of an emulator program which allow sites to be run on a computer.

Credentialed Accounts

One of the first things to look for is consent to credentialed accounts on specific platforms. Searching social media accounts with a credentialed account will yield more information. For example, obtaining consent to login to a client's Facebook account could identify private posts of their Facebook friends.

A thorough debriefing with the client is essential in gaining access to credentialed accounts as well as other potential witnesses and other areas of digital evidence.

Non Credentialed Accounts

Without the benefit of a credentialed account the search must rely on other factors and criteria. Efforts to positively identify other potential witnesses and their known associates through database and open source background searches will enhance the likelihood of locating specific user profiles.

The search for social media evidence should also include the scene or geographical area. The following example shows the results of a Twitter search by geographical area.

The approach should use a combination of open source and platform searches and document the findings using print screens pasted into a word document or saving the pages as a PDF as you go.

SEARCHING vs. PRESERVING

While this approach is acceptable for documenting the methods used to search and report the findings such as the URL address of the Facebook page, or a photo of the person for identification, the process is not considered the best practice for the actual preservation of social media evidence because of potential reliability and admissibility issues of a screen shot among other things.

The search is basically the first step needed to identify the sites by the URL address that the advanced process uses to preserve the entire site. The second step is using the advanced process to preserve the entire site, which generates hash values, obtains the metadata and imbedded content. The advance process also creates an index of the entire site that can then be search instantaneously. This capability can be a huge time saver when it comes to searching large data sets.

Basic Open Source Search Criteria

Begin the search using known information such as name, location, username or screen name, email address, physical address, known associates, photos and phone number.

Results may vary, so searches should be conducted on all three of the main search engines, Google, Yahoo, and Bing. A shortcut is to do these searches simultaneously by opening three different browser tabs and copy/paste the search criteria to each search engine.

CREATIVE SEARCH TECHNIQUES

Quotes

Use quotes to search for an exact phrase.

    Example: *"network administrator"*

Quotes and State: Use quotes to search a name by state.

    Example: *"Kevin Brown", CT*

Google's cached version of a site

Put "**cache**:" in front of the site address.

    Example: *cache:irisinvestigations.com*

Wildcard Searches:

Put an asterisk (*) in your word or phrase where you want to leave a placeholder.

Example: *"largest * in the world".*

Put **@** in front of a word.

Example: *kbrownct@twitter.*

Broaden your search with multiple terms

Put AND or OR between your search terms.

Example: *"network administrator" OR "Human Resources"*

Hash tags

Put # in front of a word:

Example: *#throwbackthursday*

Exclude a Specific Term

Put a minus (-) before the word to be excluded from your search.

Example: *administrator -manager*

Google Image Search

Right click on an image and search Google for other instances where that same image was used.

Historical Web Pages

Use an open source internet archive tool known as the Wayback Machine to search for historical web pages from when it was crawled (indexed) by the major search engines.

PLATFORM SEARCHES

Conducting Platform Searches

To conduct a credentialed account search you should obtain a signed consent from the site owner and document not only the user name and log in, but the security questions.

To conduct a non credentialed search of individual social media platforms you need to have an account profile for each one and be logged in. This means a basic understanding of each platform being used is necessary and care should be taken to avoid leaving footprints, such as viewing a LinkedIn page in public mode or inadvertently making contact by liking a post or tweet.

The searches should focus on both ownership and authorship as well as activities' at or around the time frame in question, the user's family and friends and other screen names, posts comments, photos and video etc.

Twitter

- Twitter handle
- Name
- Biographical information
- Photographs
- Any tweets mentioning them
- Location

Facebook

- Name
- Associates
- Events
- Groups
- Pages
- Hash tags

Note: Facebook updates access controls and often defaults new features to "public view" which necessitates frequent checking of preferred settings and options to maintain desired levels of privacy.

Foursquare

- Mobile only App
- Search by name, email and phone number

Instagram

- Top (All of the below)
  - People (Other users on Instagram)
  - Tags (Hash tags)
  - Places (Location tags)

Snapchat

- Mobile only App
- Phone number
- Username
- Snapcode
- Wi-Fi (if the users are connected to the same internet network).

<u>Pinterest</u>

- A profile will appear in a search engine query if they've allowed it to be indexed.
- Search Pinterest if the profile isn't indexed
- User's *Boards*, *Pins*, *likes*, *followers*, and other Pinterest users they are *following*.

<u>LinkedIn</u>

- All searches should be conducted in private mode to avoid leaving a footprint of the visit to the page.
- Name
- Employer, occupation and location

<u>Tumblr</u>

- Frequently used usernames
- Email address linked to the account
- Some Tumblr pages will integrate with the user's Twitter and Facebook accounts

DOCUMENTATION & CHAIN OF CUSTODY

One of the other challenges of conducting social media searches is how to document what was done and to preserve what was discovered.

There is a big difference between documenting the search results with screenshots, or even a PDF, and actually preserving the social media as evidence in accordance with the best practices.

When a social media search is conducted as a general background search or to identify or locate witnesses, advanced preservation methods are not always needed.

- Documenting the methods used to conduct the searches should include site URL.
- It should include a screen shot of the home page.
- It can be saved as a PDF for future reference.
- When using credentialed accounts a signed consent form should be obtained.

These steps do not capture imbedded video or active content, such as newsfeeds, and an advanced process is needed to preserve these items properly.

PRESERVATION OF SOCIAL MEDIA EVIDENCE

The most effective way to preserve evidence from the internet and social media accounts is through a forensic approach that will account for the chain of custody, authentication, and admissibility and hearsay issues. The challenge will include establishing ownership and authorship of the information in question.

The process should capture the entire page to include the metadata as well as imbedded images and videos along with active content. It should be conducted by trained personnel and in accordance with a quality management system used by the scientific community. This quality system ensures repeatable and reliable results.

- ✓ **Defensibility**
- ✓ **Reproducible results**
- ✓ **Accepted tools and techniques**
- ✓ **Proper evidence handling and documentation**
- ✓ **Objectivity**
- ✓ **Application of the scientific method**
- ✓ **Preservation of metadata**
- ✓ **Generation of hash values**

WHEN AN EXPERT IS NEEDED

When internet or social media evidence is found and is expected to be used as evidence, a trained expert is needed to preserve all of the evidence in accordance with the best practices. The process described above would be considered the minimum standard, helping to ensure the evidence collected will be admissible.

CONCLUSION

Because social media evidence will continue to be a component of every investigation and because of the possible impact it could have on the outcome of a case, it is essential to have a consistent, comprehensive approach for identifying and searching the internet while following the best practices.

Professionals should keep in mind that this evidence is fleeting and time sensitive and should be assessed, searched and preserved early on. It should be conducted on not only the involved parties, but primary witnesses, their 1st degree associates, and the scene itself.

Proper documentation should fully outline the methods used, should include site URL, a screen shot of the homepage and can also be saved as a PDF for future reference. When using credentialed accounts a signed consent form should be also obtained.

Equally important is the capability to preserve the evidence using a forensic approach that meets the standards and knowing when to get a third party expert involved.

860-522-0001

Have questions or need help on a case? Our team at I.R.I.S. LLC consists of experienced, cross-trained investigators that regularly conduct searches for internet and social media evidence, provides training to other professionals and organizations, and has the tools and expertise to preserve digital evidence using a forensic approach meeting the industry standards and best practices.