Leveraging Social Media for Investigations

Introduction

A celebrity promotes a luxury music festival to millions of Instagram followers without revealing that she was a paid promotional advertiser. A money launderer posts an advertisement on Snapchat, offering supposedly low-risk opportunities for teenagers to make some quick cash. A convicted felon is shown holding firearms in a photo on a sporting goods company's Facebook page. While superficially unrelated, what these three instances all have in common is that information posted to social media ultimately provided investigators with critical evidence in criminal and civil investigations.

Social media has transformed the investigative landscape for public and private investigators. **Social media — and the data it captures — has played a key role in the investigative process for cases involving fraud, defamation, disinformation, counterterrorism, compliance, privacy, blue- and white-collar crime, financial crimes, and civil litigation**. As social media has continued to blend together people's public, private, physical, and online lives on a daily basis, the process for collecting evidence, identifying leads, identifying individuals, assets, and known associates, and investigating a case has become increasingly dynamic. Thus, for today's investigator interested in staying ahead of nebulous cases or nefarious actors, she or he must constantly adapt to find, analyze, and operationalize relevant and timely information.

Social media intelligence (SOCMINT) refers to the process of identifying, collecting, and analyzing data generated by organizations' and individuals' use of social media and other digital platforms to post information, discuss topics of interest, and generally navigate their online needs. SOCMINT covers the full information spectrum, including written, audio, and visual content. **SOCMINT leverages an organization's or individual's online footprint to identify trends and anomalies in online behavior, based on post content, frequency, identified interests, news preferences, emotional sentiment, geographic and demographic data, searches, social and professional networks, and financial activity.**

In conjunction with other open-source data, **SOCMINT can serve as a force multiplier for investigators by enabling them to cast a wider net than more siloed research approaches.** Social media platforms regularly encompass public and private data because organizations and individuals frequently interconnect their social media accounts with other types of accounts for simplicity and better functionality.

Oftentimes social media can create an enduring archive of an individual's life — including an individual's posts, interactions, interests, photos, videos, and locations and demographic data. This data allows investigators to learn more about a subject of interest. SOCMINT can also help investigators track trends and identify potential anomalies in public conversations about an organization's events, brands, and products.

Guidehouse's Broader Open Source Intelligence (OSINT) Capabilities

While SOCMINT can offer a novel investigative approach, social media represents only a portion of the investigative cycle and resources available today. Guidehouse's Open Source Solutions team has extensive experience and expertise in open source investigations. Our team has a deep, diverse, and ever-expanding set of domestic and foreign information sources based on publicly available information and commercially available data sets. We integrate these sources with OSINT tools and capabilities to develop information on subjects of interest and to fulfill investigation requirements. Our team can leverage the full spectrum of sources — traditional and non-traditional media, user-generated content, professional and academic sources, public data, company filings and records — to ensure investigations are built on a comprehensive, timely, and accurate basis of facts. Guidehouse's strategy, sources, methods, and tradecraft are expertly tailored to the scale and scope of each investigation to balance investigative agility with secure protocols.

Monitoring the Indexed and Unindexed Internet

In addition to monitoring traditional and social media platforms, Guidehouse can also employ its darknet-monitoring capability as a part of its SOCMINT services to collect, analyze, and visualize data from illicit forums, marketplaces, chat services, blogs, paste sites, card shops, and other sources. This deepens our team's ability to identify critical pieces of information relevant to investigations.

An Overview of the SOCMINT Ecosystem		
Resource Type	**Sources & Tools**	**Types of Information**
Primary	• Common Social Media Platforms (e.g., Twitter, Facebook, & Instagram) • Less Common Social Media Platforms (e.g., Telegram & WhatsApp) • Desktop, Mobile, & Tablet Apps • Social Media & Network Analysis Tools	• Contact Information (e.g., email & phone) • Alternative accounts, organizations, & assets on the Indexed & Unindexed Internet (e.g., potential straw owners and shell companies) • Social & Professional Networks
Secondary (When Applicable)	• Traditional Media Platforms • Forums, Blogs, & Paste Sites • Cryptocurrency Networks & Other Marketplaces • Darknet • Global Business Findings & Records • Public & Private Databases • Open-Source Analysis Tools & Mapping Platforms	• Post Content, Frequency, & Emotional Sentiment • Conversational Trends & Anomalies (e.g., trending hashtags) • Photos & Videos • An Individual's or Organization's Identified Interests & News Preferences • Geographic, Demographic, & Financial Data

While some public and private-sector organizations have begun to incorporate SOCMINT into their investigations, many are still approaching SOCMINT in an ad hoc way. Exploiting the fluid social media landscape can seem like a daunting process, but success in this field can develop leads for new investigations and add additional depth to existing investigations. **Proactively exploiting social media can be the difference between finding or missing a key connection that ties together seemingly unrelated pieces of evidence in an investigation.** Indeed, careful and qualified SOCMINT can be leveraged to provide immediate operational impact for investigators.

Guidehouse's Unique Approach to Supporting Investigations with SOCMINT

in close coordination and collaboration with clients, Guidehouse implements a four-step approach to conduct SOCMINT in support of our clients' investigations:

1 **Define the SOCMINT scope.** Our team works with our clients to create targeted SOCMINT plans that address the investigations' specific objectives, priorities, deadlines, actors, and resources, while also accounting for — and mitigating — investigative risks.

2 **Collect, organize, and preserve publicly available social media data.** Our team configures and deploys appropriate tools, methods, and tradecraft for ensuring and maximizing the quality, objectivity, utility, and integrity of the collected information. Data collection and organization are tailored to the scale and scope of each investigation. Data preservation is based on appropriate tradecraft, as well as the investigation's intended audience

3 **Analyze the data and refine it into intelligence.** Our team exploits the collected social media data to identify trends, anomalies, leads, sources, and risks that are consistent with the scoped investigation. This could include drilling down on an individual's or organization's social and professional networks, emotional sentiment, posted content, photos and videos with geolocation potential, and geographic, demographic, and chronological data. This intelligence can encompass conflicts of interest, unreported financial and travel activity, alternative social media accounts, straw owners and shell companies, and new witnesses, obstacles, and pieces of evidence.

4 **Report SOCMINT findings and highlight additional opportunities for finding relevant data.** Our team synthesizes the intelligence into concrete findings for investigators and highlights additional areas where SOCMINT could further support the investigation.

How Can Guidehouse's SOCMINT Capability Benefit Your Investigation?

Guidehouse has the tools, technology, and expertise to expand the aperture of our clients' investigations by tapping into social media. We offer the following SOCMINT services in support of a diversity of investigation types:

Corroborate or refute existing information: Perform preliminary checks on statements and accusations to determine if they can be corroborated or require more resources.

Launch new investigations: Use publicly available social media data to evaluate existing witnesses and evidence and address investigative gaps.

Assess social networks: Utilize social media data to map out key actors in an individual's or organization's network and measure the type, strength, frequency, and content of their interactions. For instance, investigators could employ social network analysis to better understand a criminal organization with an obscure structure. Analyzing the network's interactions could result in identifying derogatory information or the crime boss and his lieutenants, as well as their couriers, accountants, and other staff.

Enhance and expand traditional asset tracing: Use a subject's social media footprint to enhance and expand on asset tracing based on traditional means of analyzing a subject's ownership of assets (e.g., real and personal property), travel patterns, and financial operations. The process seeks to identify potential conflicts of interest and inconsistences in the subject's reported and unreported activity in these three areas. Geolocation and social network analysis can then be implemented to uncover potential straw owners, shell companies, and various types of misconduct.

Track and analyze online trends and anomalies: Leverage unique methodologies and SOCMINT tools to track and analyze trends and anomalies in online activity relevant to the investigation.

Identify and monitor threats and risks: Monitor social media and digital sources for emerging red flags, threats, and vulnerabilities for the investigation. Threat detection identifies potentially hostile actors and assesses how they may pose risks to the physical and electronic security of investigators, witnesses, and evidence.

Provide advisory services: Provide guidance on the designs, approaches, and benefits of specific investigations and identify additional research opportunities where social media, darknet, and other types of data could further support the investigation.

Why Guidehouse

Guidehouse delivers actionable solutions that enable our clients to identify and overcome investigative gaps and obstacles, locate and evaluate witnesses and pieces of evidence, and confirm that their findings are timely, accurate, and comprehensive. Our focus on quality through execution brings forth the best and brightest minds to support projects that yield impact. This, in turn, fosters insight and innovation to approaching dynamic challenges. Our clients rely on Guidehouse not only because we provide strategic and operational recommendations based on reliable, near-real-time data, but also because our guidance leads to informed decision-making, actions, and high-impact solutions. Guidehouse provides best-in-class SOCMINT capabilities that enable investigators to apply innovative techniques that can anticipate and navigate the ever-changing social media environment. We work with our clients to determine how social media can amplify and enhance existing investigations or jump-start new ones.