Social Media Awareness for Enforcement

IALEIA

Professionalizing Intelligence Analysis Since 1981

Booklet Committee:

Marilyn B. Peterson
Tracy Lempke
Lynn McCloskey
Alison Price-McGinnis
Jenny Urquhart

Table of Contents

Introduction 4

What Social Media Are and How We Can Best Utilize Them 4

Top Social Media Sites 5

How Social Media Assist Law Enforcement 7

Criminals on Social Media 8

The Dark Web and Tor 9

Enforcement Considerations Regarding Social Media 10

Disinformation and Memes 11

Some Current Social Media Exploitation Software 12

Case Examples 15

Value-Added Analysis 16

Social Media Resources 17

Some Social Media Terminology 18

References 20

IALEIA 22

Introduction

Social media and their exploitation, or analysis, by law enforcement and national security is not a new investigative technique. However, some managers, leaders, investigators, and analysts are unsure of what the terms mean and how to do them. The purpose of this booklet is to provide a basic overview of the concept and techniques. In addition, there are tools that can assist in reviewing and analyzing social media data. This booklet will also inform leaders and managers of how analysts are integral to social media exploitation. The challenge with these sources of information, tools and investigative/analytical techniques is that the landscape, tools, and trends change daily. This is one snapshot in time and IALEIA will periodically update the information contained in this booklet

What Social Media Are and How We Can Best Utilize Them

Social media are internet-based forms of communication that allow users to have conversations, share information, and create web content. Media exploitation refers to the extraction, translation, and analysis of media to generate useful and timely information (Technopedia 2022). There are many forms of social media, including blogs, micro-blogs, wikis, social networking sites, photo-sharing sites, instant messaging, video-sharing sites, podcasts, widgets, virtual worlds, and more (USF 2022). The estimated total global population using social media is 4.59 billion users, or 56.8% (Staistica 2022).

About 70% of Americans have used social media, according to the Pew Research Center. The highest category of users was women (78%), between 30 and 49 years old (77%), Hispanic (80%), earning over $75,000 per year (78%), having a college degree (77%), and living in an urban setting (76%). The least category of users was men (66%), over 65 years old (45%), white (69%), earning between $50,000 and $75,000 (65%), having a high school degree or less (64%), and living in a rural setting (67%) (Pew Research 2021).

Today's technology is increasingly accessible to the average law enforcement organization. "Responsible access and analysis of these technologies hold promise for identifying and halting crime threats, investigating crimes and holding offenders responsible, and detecting and responding effectively to emergencies and hazards (all of which are core objectives of law enforcement… At the same time, law enforcement access to and analyses of communications data raise concerns about, and require protections for, individual privacy, civil rights, and information security" (Hollywood et al. 2018, p. 3).

The volume and range of information posted to social media make these platforms both a challenging and ideal place for intelligence collection. For example, Twitter users send 867 million tweets per day, up from 500 million in 2015. (Yacub M. 2022; Whitney 2022). Users post photos, videos, and status updates to social media, and their profiles often include such personal details as their age, gender, family members, and place of employment. These posts offer insight into the daily lives of individuals, as well as the attitudes and behaviors of social networks. It is now widespread practice for major companies to use social media analytics to better understand their customer base, guiding marketing decisions and product development (interview with subject-matter expert, September 1, 2016 (Marcellino, Smith, Paul and Skrabala 2017, p. 10).

Maltego's *Handbook for Social Media Investigations* details how to gather and collate the information found on these sites. It shows how beginning from a name, an alias/username, a phone number, an image, an address, or location you can build information not only on the original target, but on people, locations, businesses, and organizations in the target's network (2022, pp. 13 – 26).

Top Social Media Sites

The most popular social media site are shown below, so one can explore them as needed. The list is from: www.simplilearn.com/real-impact-social-media-article#top_7_impacts_of_social_media

Facebook/Meta

Facebook (Meta) is one of the original social media sites launched in 2004. Users can post live video, photos, messages, celebrate birthdays, etc. It has 2.91 billion users. www.facebook.com

TikTok

TikTok shares short videos posted by users to its 1 billion user audience. It combines graphics with action videos to interest its followers. www.tiktok.com

Instagram

Instagram is a simple, fun, and creative way to capture, edit and share photos, videos, and messages. It has 1 billion users. www.instagram.com

Pinterest

Pinterest is a search engine for finding ideas like recipes, home, style inspirations, and more. Pins are bookmarks that people use to save content they like such as images, videos, or products. It has 431 million users. www.pinterest.com

Reddit

Reddit is a website that aggregates social news and discussion. It was founded in 2005 and has 330 million users. Varied communities and groups share postings on it. www.reddit.com

YouTube

YouTube is a leading video outlet that has music, gaming, sports, news, learning and trending material that 2.6 billion users watch. It includes channels that users can subscribe to as well as a library of videos.
www.youtube.com

WhatsApp

WhatsApp provides free messaging through a phone's internet connection, allows shared messages, photos, and videos of up to 256 people at once, and gives face-to-face conversations via the phone's internet connection. It has 2 billion users with many users in India and Africa. www.whatsapp.com

Twitter

Twitter provides breaking news, entertainment, sports, politics, and opinions. It has a limit to messages but allows one to link messages for more in-depth data. It had 330 million active monthly users in 2020. twitter.com

LinkedIn

LinkedIn is a platform that highlights professional relationships and has postings including job openings, job shifts, training, and organizational news. There are sub-sites one can initiate or join along with 66.8 million other users. www.linkedin.com

Snapchat

Snapchat is a Social Media site devoted primarily to pictures or video with the creative ability to alter the images to create an augmented reality. It has 293 million users. www.snapchat.com

How Social Media Can Assist Law Enforcement

Social media are both a boon and a problem for law enforcement. While they can help policing efforts, they also create new technological challenges for law enforcement. "Thanks to social media, law enforcement has an unprecedented opportunity to communicate directly with the community and help shape an accurate depiction of events in the midst of crises" (Pennybacker and White 2021, p. 5) That "accurate depiction" is key in times when some find it hard to separate fact from fiction. But "…by leveraging the power of a credible social media voice, law enforcement liberates itself from the media's interpretation of events" (Pennybacker and White 2021, p. 1).

Spiliotopoulou et al. referred to the opportunity as "government as a platform (having a government-to-citizens (G2C) orientation government provides to citizens extensive information and knowledge to assist them to improve their well-being and productivity…" (2014, p. 548). They suggested simultaneous use of multiple platforms to reach a wide audience, publishing public policy-related content and monitoring citizens' interactions with the content, and analyzing those interactions to extract levels of public support (p. 552).

Several cases point to the effective use of social media. "The Boston Marathon bombing incident (2013) showed both law enforcement and the public that verified law enforcement information can be channeled directly to the public…" (Pennybacker and White 2021, p. 3).

Federal Bureau of Investigation (FBI) use of Twitter during crises is a case in point. High-profile shootings at an El Paso (TX) Walmart and the Virginia Beach (VA) municipal building are two 2019 examples. "In each case, as soon as FBI assets were deployed, a public affairs specialist used Twitter to establish the office as a beacon of source-verified information. The FBI understood the value of telling its story using Twitter without compromising any future criminal investigation" (Pennybacker and White 2021, p. 3).

Police agencies have noticed and analyzed the social media impact. "In the Urban and IACP survey, respondents indicated that they use social media for a variety of purposes, the most common being to notify the community of public safety concerns (91%). They also reported using social media for community outreach and citizen engagement (89%), public relations and notifying the community of non-crime issues (86%), soliciting crime tips (76%), monitoring public sentiment (72%), intelligence gathering for investigations (70%), and recruitment and applicant vetting (58%). In addition, 60% of agency respondents indicated that they had reached out to a social media company to request information to use as evidence" (Congressional Research Service 2022, p. 1).

Social media can also help to strengthen bonds between police and the community. "Broadcasting live content through both Instagram and Facebook is a pivotal strategy for law enforcement to forge connections with constituents and strengthen community engagement by having conversations in real-time…being transparent on social media is key to law enforcement agencies in today's sometimes hostile landscape as it provides a space for all to socially connect and share their story" (Law Enforcement Social 2020).

Criminals on Social Media

While most users of social media are everyday people "…social media can facilitate injurious forms of social interaction, such as sexting, online stalking, and cyber-bullying" (Obar and Wildman 2015 p. 16). Commonly reported crimes that occur on social media involve people making threats, bullying, harassing, and stalking others online.

Although logging into a friend's social media account to post an embarrassing status message may be forgivable between friends, it, technically, can be a serious crime. Additionally, creating fake accounts, or impersonation accounts, to trick people (as opposed to just remaining anonymous), can also be charged as fraud depending on the actions the fake/impersonation account holder takes.

Connecting over social media to make business connections or buy legal goods or services may be perfectly legitimate. However, connecting over social media to buy drugs, or other regulated, controlled, or banned products is illegal. More and more criminals are posting videos of their crimes on social media. This is short-sighted as police departments and prosecutors can use videos to arrest and convict criminals.

One common practice among burglars is to use social media to discover when a potential victim is on vacation (Thomson Reuters 2022). It has been found that "…apps can also be installed on laptops, computers, game consoles, wearable devices (such as smartwatches or fitness trackers), smart TVs, smart speakers (such as Alexa devices), and IoT (Internet of Things) devices…In one example, a security company showed it could create and link a malicious app for a popular tracker that contained spyware able to steal locations and personal body data" (BBC 2022a).

Although Russia has denied it harbors cyber-criminals, researchers say that $400 million worth of ransomware in 2021 went to Russia-linked hackers. They followed the money to and from digital wallets of known hacking groups using public blockchain transaction records (BBC 2022b).

"A blockchain is a distributed database or ledger that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. Blockchains are best known for their crucial role in cryptocurrency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions" (Investopedia 2021).

In his dissertation, Ekunwife noted that "increased social media usage aligned with the increased numbers of mass shooting incidents (and) some users of social media platforms share data that may have mass-shooting-incident-related content that other users may copy and later act upon" (2022, p. 10-11).

In February 2019, three men followed Abel Mosso into a New York City subway station. Two of the men, alleged associates of MS-13, attacked Mosso inside a subway car before dragging him onto the platform. There, the third man, an alleged member of MS-13, warned bystanders not to interfere by shouting, "Nobody get involved, we're MS-13, we're going to kill him." He then shot Mosso multiple times in the head. Investigators found a video on Facebook of the murder...The video was later used as evidence when the government charged the three men with murder in aid of racketeering and intentionally discharging a firearm during a crime of violence (Degani 2021).

The Dark Web and Tor

Tor is an acronym for "The Onion Router" and is an ope-source software that enables anonymous communication. It currently has about 2 million users predominantly from the United States, Germany, and Russia (Trulist 2022). Using Tor through a Virtual Private Nework (VPN) connection allows users to conceal their device's Internet Protocol (IP) address.

Tor itself is not illegal; however, it is used to access the dark web and operate services anonymously. Because of this anonymity, the frequently hosts illicit content such as the online marketplace, "The Silk Road." The FBI shut down The Silk Road. It subsequently re-opened under the name "Agora" which was shut down in 2015. It was followed by the AlphaBay black market site which was shut down in 2017 (Economist 2017).

The dark web has search engines that are only accessible using Tor, including:

Ahmia
juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4cysd.onion/
This is a list of Tor sites that do want to be found.

Haystak
haystak5njsmn2hqkewecpaxetahtwhsbsa64jom2k22z5afxhnpxfid.onion/
Like Ahmia, Haystak also uses a custom dark web crawler and filters out dangerous content.

Torch
xmh57jrknzkhv6y3ls3ubitzfqnkrwxhopf5aygthi7d6rplyvk3noyd.onion/
Torch is one of the oldest and most popular search engines on the dark web, serving over 80,000 requests per day.

DuckDuckGo (also accessible on the open net)
duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/
The internet's favorite alternative to Google made a name for itself by not logging search activity yet still providing decent results. This focus on privacy makes it the Tor browser's default search engine. It does not search onion sites. (Express VPN 2022). Onion sites are those that are found in the .onion domain

Enforcement Considerations Regarding Social Media

The International Association of Police Chiefs (IACP) developed guidance for law enforcement agencies regarding social media in 2019. Its suggestions were as follows:

"Social media" can be used

1. As an investigative tool when seeking evidence or information about
    - Missing persons,
    - Wanted persons,
    - Crimes perpetrated online (e.g., cyberbullying, cyberstalking), and
    - Photos or videos of a crime posted by a participant or observer.
2. For community outreach and engagement by
    - Providing crime prevention tips;
    - Offering online reporting opportunities;
    - Answering questions posted by the community on social platforms;
    - Sharing crime maps and data;
    - Providing a two-way tool to enhance and promote community trust building; and
    - Soliciting tips about unsolved crimes.
3. To make time-sensitive notifications related to
    - Road closures,
    - Special events,
    - Weather emergencies, and
    - Missing or endangered persons.
4. To inform the media by
    - Becoming a source of information immediately following a critical incident,
    - Dispelling rumors and corrected misinformation, and
    - Magnifying the agency's message and instructions when media reshares on their own "social media platforms" (IACP 2019, p. 2).

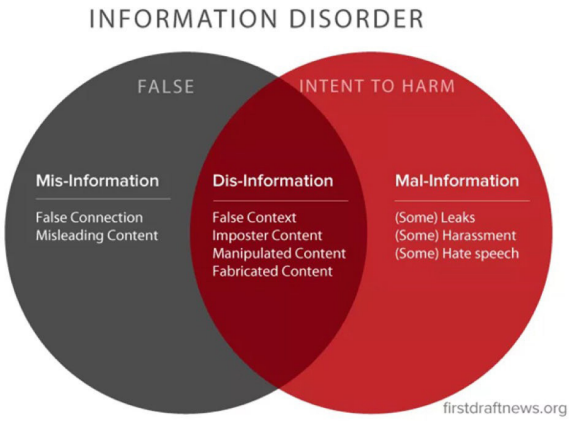
This advice encourages informed use of social media with an awareness of its positive attributes that can be helpful to agencies of any size. (Material reprinted with written permission from IACP.)

U.S. Department of Justice 2018 policy states that: "Social media tools provide the technical capability to communicate and disseminate information to the public on behalf of the Department of Justice (DOJ or Department). The Department permits components to use social media tools, conditioned on appropriate approval, to provide information and enhance communication with the public in support of DOJ's mission when such use:

- promotes the mission, goals, and objectives of the Department;
- complies with applicable statutes, regulations, Federal Government-wide guidance, and departmental policies;
- protects individual privacy;…
- complies with applicable ethical standards;…
- operates only under Terms of Service (TOS) agreements that have been reviewed and signed by a Department official to ensure compliance with federal laws; and
- is authorized by the Department's Social Media Working Group (SMWG) and man aged in accordance with this Policy Statement..." (U.S. DOJ 2018, p. 6).

Disinformation and Memes

Many researchers caution using data from social media sites because sources can be unclear or unreliable. One study recent study saw that the percentage of people in 36 countries relying on social media as a primary source of news was 54% (Muhammed et al. 2018).



Source: C. Wardle & H. Derakhshan 2017, p. 5

"…Facebook states that its News Feed prioritizes recent content that is found to be relevant to the user, based on factors such as previous engagement with the content provider. The algorithms also may prioritize content that is likely to sustain user engagement—such as sharing, commenting on, or reacting to content—rather than the content's veracity. According to a *Wall Street Journal* article, slides presented by an internal Facebook team to company executives in 2018 stated, "Our algorithms exploit the human brain's attraction to divisiveness," and warned that the algorithms would promote "more and more divisive content to gain user attention & increase time on the platform" (Horwitz and Seetharaman 2020).

Three tactics characteristic of extremist online communities:

- They use memes as propaganda,
- They employ sophisticated communications networks, and
- They organize militias and inspire lone wolf actors (Finkelstein, et al. 2020).

Memes are graphics or photographs that are satirical or funny but can also inflict great harm.

During the summer of 2020, a disinformation attack against online retailer, Wayfair, claimed that cabinets sold with female names had been used to traffic females. Wayfair's CEO received hate mail and the company had significant negative attention (Gips and Goldenberg 2021, pp. 21-22).

Far-right extremist, Nick Fuentes, uses cartoonish memes to spread white supremacist views. He uses irony and jokes to spread his message without consequences. On one of his shows, he went on a violent and misogynistic rant, only to then say "just joking." He has also said that "Irony is important for giving cover and plausible deniability for our views" (NPR 2021).

Gips and Goldenberg commented that "Lies now circumnavigate the globe, ricochet incessantly, intermesh inextricably with truth, seed institutional distrust, torpedo brand value, destroy corporate reputations and queue up to repeat the process" in quick succession (2021, p. 2).

Some Current Social Media Exploitation Software

This field expands daily, with more companies developing or partnering with social media exploitation software. The below list shows some that are available but does not represent the totality of current software, nor does it imply an endorsement by IALEIA.

Babel X www.babelstreet.com/platform/babel-x
Babel X canvasses publicly and commercially available information across more than 200 languages and then filters it by geospatial, temporal, link analysis, public records search, sentiment, and topics of interest. Results are presented on a single pane of glass for analysis and collaboration.

Blue Light www.bluelightllc.com
Blue Fusion allows the client to ingest and aggregate structured and unstructured data regardless of location, format, or structure into a scalable, multi-user database environment on the cloud or on-premise.

Cobwebs cobwebs.com
The Cobwebs web investigation platform is powered by Artificial Intelligence (AI). It enables the search of online data using machine learning algorithms in both the open and dark webs.

Fivecast www.fivecast.com
Uses AI-enabled technology to solve complex intelligence challenges. Has threat, image, and video analytics along with deep learning and network analysis.

GeoTime www.geotime.com
GeoTime includes a suite of products that can communicate data with investigators, analysts and in the courtroom to judges and juries.

I2 Group www.i2.com
I2 offers the Analyst's Notebook and related software. It is available with 'plug-ins' for social network analysis and content analysis.

Kaseware www.kaseware.com
Kaseware is an investigate platform that manages cases, records, and evidence. It provides dashboards, link analysis and evidence management. It partners with Shadow Dragon.

Logically www.logically.ai
Threat intelligence and fact-checking capabilities available to organizations globally. It uses Extended Intelligence to explore today's media landscape.

Maltego www.maltego.com/
Maltego Machines automate standard or repetitive investigative steps. They allow users to increase the process of data collection and allocate more time to analyzing an automatically populated graph.

Media Sonar mediasonar.com
Its investigative module, Pathfinder, empowers novice and experienced teams with the ability to use open and Dark Web tools in a single platform

Ntrepid ntrepidcorp.com/
Supports managed attribution in law enforcement open-source intelligence.

PenLink PLX www.penlink.com
The PenLink company has provided communication analysis software and reporting for several decades. Today, it can collect, analyze, and export large volumes of social media, email, and other internet communications data.

Rosoka www.rosoka.com
Rosoka is a plug-in to the i2 software which allows natural language extraction in 200 languages.
It focuses on rules-based and machine learning algorithms to identify, geo-tag and focus on relationships including salient scoring and sentiment analysis.

Scam Search www.scamsearch.io
A free service that is a database of Crypto scams, email, social networks, offline scams, phone scams, literally every single scam situation you can think of, this site records it and makes it available. They currently have 10 million recorded scammers and it grows weekly by several thousand.

Shadow Dragon shadowdragon.io/
SocialNet is for social media monitoring and investigations. It captures the digital tasks of criminals, maps it against their aliases and looks at their connections in real time to expedite investigations.

Skopenow www.skopenow.com
Skopenow builds comprehensive digital reports collecting and analyzing publicly available data from social media, the dark web, court records, and contact data.

UserSearch www.usersearch.org
UserSearch is a network of search engines that crawl the web to find an exact match on a username or email address. It scans across hundreds of websites. It can locate a particular user profile on forums, social networks, dating websites, message boards, crypto websites, and gambling websites. The basic version is free.

VA Insight www.vainsight.com
VA Insight has a browser-based platform that streamlines data collection and provides tactical visualization to deliver operational intelligence to officers.

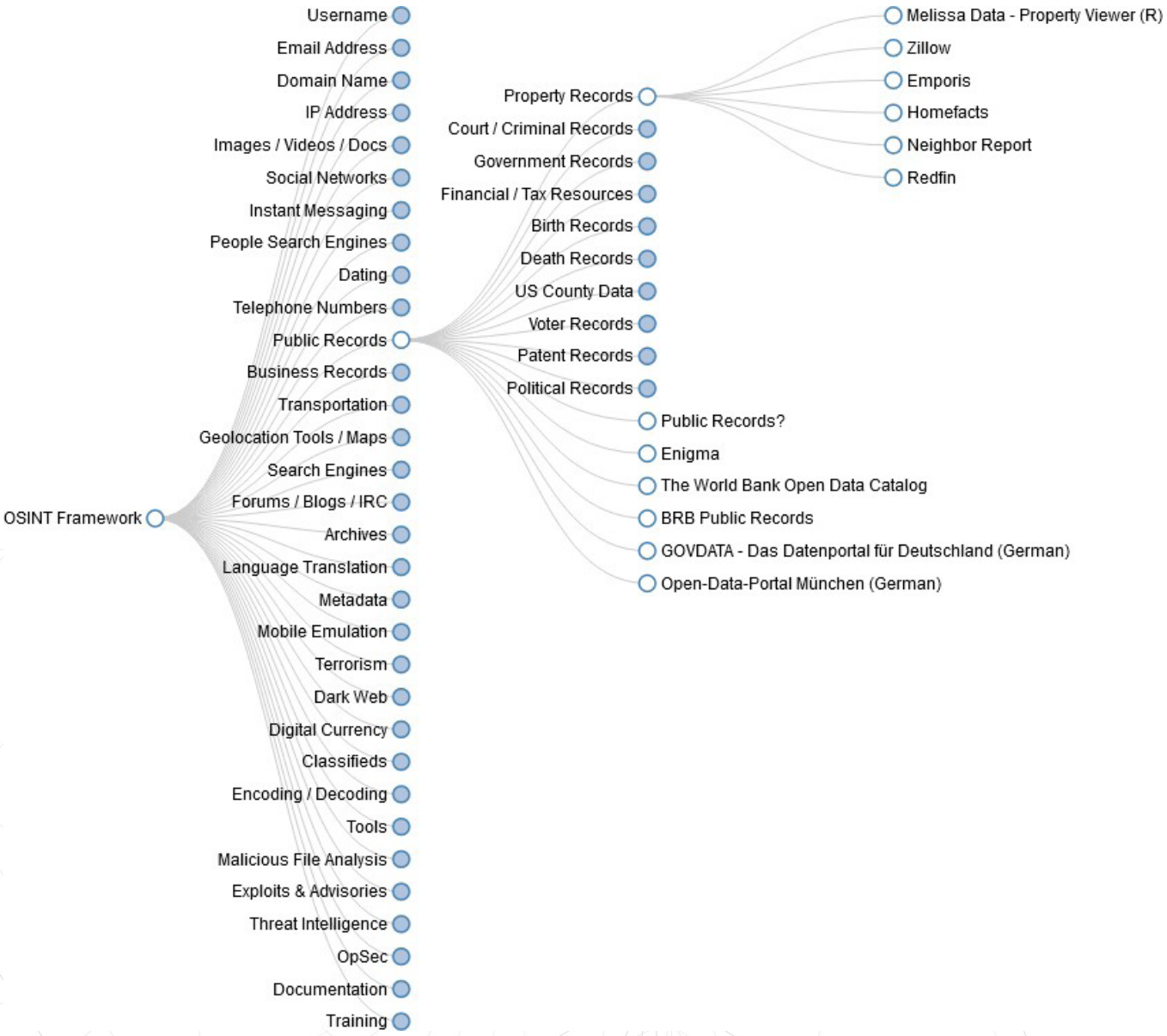
Whooster www.whooster.com
Whooster offers advanced data fusion and analytic technology.

OSINT Framework osintframework.com/

This site allows you to drill down on varied types of sites to get specifics on what you need.

The OSINT framework focused on gathering information from free tools or resources, to help people find free OSINT resources. Some of the sites included might require registration or offer more data for $$$, but you should be able to get at least a portion of the available information for no cost.

Watch the project on Github: github.com/lockfale/osint-framework.



Case Examples

In 2015, a young woman was found dead on the side of the road in Saskatoon, Canada, with a belt near her body. Three years later, Saskatoon police convicted Cheyenne Rose Antoin of manslaughter based on a photo Antoin posted on Facebook of her and the victim taken earlier on the night of the victim's death. The police were able to show that the belt Antoin was wearing in the photograph was the same one left at the scene of the crime. Police may never have been able to link Antoin to the crime without that Facebook photo (ThomsonReuters 2022).

The National Intellectual Property Rights Coordination Center (IPR Center) joined 94 Interpol member countries in a crackdown on illicit online pharmacies June 23-30, 2022. The operation netted more than 7,800 seizures of illicit and falsified medicines, totaling more than three million individual units at $11 million. Advertisements for medicines invade the Internet, posted on social media networks or other websites. The global trade in illicit pharmaceuticals was valued at $4.4 billion in 2016 and attracts the involvement of organized crime groups around the world (U.S. Customs and Immigration Enforcement 2022).

A former Jacksonville (FL) second grade teacher pled guilty to distributing child sexual abuse videos using a social media application in 2021. The company owning the social media messaging application saw videos depicting child sex abuse and notified the National Center for Missing and Exploited Children which led to his arrest. The teacher faces between 5 and 20 years in federal prison for his activity (U.S. Attorney's Office 2021).

Two Nicholasville (KY) men were sentenced in 2018 for using social media to harass and intimidate an acquaintance with threats of a prospective shooting at a Jessamine County school. One received 21 months in federal prison and the other received 27 months in federal prison. Each pled guilty, in June 2018, to one count of cyberstalking. They had worked together to create a Snapchat profile using the name and picture of a third person who did not know about their actions. They then used the profile to publish a series of posts suggesting that this third individual would use firearms to attack a Jessamine County public school (U.S. Attorney's Office 2018).

Two Washington, DC men were indicted by a federal grand jury in 2021 for a violent kidnapping live-streamed on social media. They were charged with conspiracy to commit kidnapping, kidnapping, and cyber stalking. The investigation began after officers became aware on January 24, 2021, of a live stream on the Instagram showing an injured and distressed adult male being held against his will and assaulted. The defendants were alleged to have violently assaulted the victim, on January 23, 2021, with a variety of implements, including an electrical extension cord, all while broadcasting their actions on social media. Metropolitan (DC) Police Department officers apprehended both defendants on the scene and recovered a firearm (U.S. Dept. of Justice 2021).

One company was targeted by hackers who wanted to steal critical and sensitive data. With the Digital Risk Protection program, an analyst was able to identify their digital footprints in a non-intrusive way. They were also provided with real-time notification of malicious chatter and attacks related to COVID 19 and the company. They were then able to remove the malicious content, mitigating similar attacks (Cobwebs 2022).

Value-Added Analysis

Analysts have long been the translators of materials foreign to law enforcement executives, whether these were in a different language, a wiretap audiotape, a type of data, or from some sources in academia. In social media, analysts initially mine the data and opinions in the media. Spiliotopoulou, et al. (2014) notes that this requires three tasks:

Classification of an opinionated text,
Classification of each sentence in such a text to determine if they reflect opinion, and
Extraction of specific issues within the text and identification of the orientation of the author.

So, too, can they translate data found in social media to inform law enforcement about activities and plans that may be a threat to life and property. Without analysis, information from social media remains just that – unconnected and unevaluated facts that accumulate in a data base with no relationships or meanings.

There are five primary analytic techniques that can be used in social media exploitation: communications analysis, content analysis, geospatial analysis, network analysis, and social network analysis.

Communications analysis is the review of records reflecting communications (telephone, e-mail, text messaging, social media postings) among entities for indicators of criminal associations or activity. collection and analysis of the metadata that results from a communication (Global Justice 2012, p. 27). This can include date, time, initiator, recipient, and length of time in the communication. This is a law enforcement technique that has been useful for decades. It can reflect activity leading up to a criminal event and may uncover the breadth of the criminal organization over time and geography.

Content analysis is used "to infer the importance writers, producers, media, or even whole cultures assign to particular subject-matter categories from the frequency or volumes with which such subject matter is mentioned" (Krippendorff 1989, p. 403). This includes uncovering the significance and the sentiment behind the posting, its propaganda value as well as analyzing the data for relationships and their meanings. Content analysis of postings can show intentions and plans of potential terrorists or criminal actors as well as leadership and influencers.

Geospatial (geographic) analysis is an evaluation of the locations of criminal activity or criminals to determine whether future criminal activity can be deterred or interdicted through forecasting activity based on historical raw data (Global Justice 2012, p. 29). Social media can reflect locations through a user posting photographs, providing a narrative while on a trip, or commenting on their location.

Network analysis (a.k.a association analysis) is the collection and analysis of information that indicates relationships among varied individuals suspected of involvement in criminal activity and providing insight into the criminal operation and which investigative strategies might be the most effective (Global Justice 2012, p. 27). It can include the connections among people, locations, businesses, organizations, or activities.

Social network analysis (SNA) is a research method developed primarily in sociology and communication science, and focuses on patterns of relations among people and among groups such as organizations and states (Vaughan 2005). Its algorithms have been incorporated into numerous network analysis programs to allow analysts to use both network and SNA tools to delve into social media data.

Social Media Resources

To learn more about social media practice, there are courses, papers, and conferences available as shown below.

Advanced Social Media Certification Training
www.simplilearn.com/learn-social-media-basics-skillup?term=advanced%20social%20media%20program

Agency for International Development (AID) and Consortium for Elections and Political Process Strengthening (CEPPS)
Countering Disinformation counteringdisinformation.org/index.php/

Cybersecurity and Infrastructure Agency (CISA)
Mis-, Dis-, and Malinformation Resource Librarywww.cisa.gov/mdm-resource-library

Federal Law Enforcement Training Center course
Digital Evidence Collection in an Enterprise Environment (11 days)
www.fletc.gov/digital-evidence-collection-enterprise-environment

International Association of Chiefs of Police
Social Media Considerations (paper)
www.theiacp.org/sites/default/files/2019-05/Social%20Media%20Considerations%20-%202019.pdf

National White Collar Crime Center courses (NW3C.org)
CI102 Basic Cyber Investigations: Dark Web & Open-Source Intelligence (3 days)
CI107 Deepfakes: An Introduction to Synthetic Media (online)
CI131 Introduction to Social Media and Networking (online) CI134 OSINT Module 3: Social Media Searching (online)

National Risk Management Center (NRMC)
NRMC is the planning, analysis, and collaboration center within the Cybersecurity and Infrastructure Security Agency (CISA), leading strategic risk reduction efforts for the United States. It works with public and private stakeholders to manage these risks. www.cisa.gov/nmrc

Network Contagion Lab at Rutgers University
This organization has authored numerous reports on disinformation, including "Emerging Threats from Extrem ist Behavior and Disinformation". networkcontagion.us/reports/

Some Social Media Terminology

Social Media use numerous abbreviations and terms which may not have been encountered in general life. Here are some that may be helpful.

AI Artificial intelligence (AI) is used in many social media exploitation programs to assist in gathering and integrating results.

Archive While a 'story' might disappear from Instagram 24 hours after it is posted, old stories can be found using Instagram's Archive tool.

Challenge A TikTok challenge is encouraging other users to record themselves doing a specific thing or action, like the intuition challenge.

Cheugy A word used to describe a person who follows out-of-date trends (fashion, decorations, social media captions, etc.). It's another word for basic.

DM Direct message: A private message on social media

Double tap A double tap refers to the action of double tapping or clicking on a post on Instagram or TikTok. Users can double tap instead of physically pressing the like "or " " button.

Gallery This is Instagram's term for a "photo album."

IB Inspired by. Another way to give credit to a content creator, especially on TikTok.

IoT Internet of Things. Computer capabilities found inside cars, watches, appliances, manufacturing, medical items, etc.

Meme A humorous image, video, piece of text, etc., that is copied (often with slight variations) and spread rapidly by internet users.

Micro blog A blog with a limited number of characters allowed, such as Twitter, which allows 280 characters.

Mini blog A blog larger than the Micro blogs, up to 2,000 – 3,000 characters.

OOMF "One of my followers" Used often on TikTok.

PFP "Profile picture."

Pinned post When a user or creator pins a post, the social media platform keeps the post at the top of the user's account, so when others visit their profile, it is the first post they see. It is used often on Facebook, Twitter and TikTok.

Podcast A short audio broadcast on the internet that may be part of a series to which one can subscribe.

Pwn To have power or mastery over someone.

Reactions Facebook introduced reactions to give users more options than just "liking" a post. Reactions include: *like, love, care, haha, wow, sad and angry.*

Shadow banned Being shadow banned means a social media platform, like Instagram, is limiting or restricting content created by a user without the user knowing. This usually happens when a user has violated community guidelines, or their content is viewed as inappropriate.

Thread Twitter allows users to create threaded tweets, which are a series of connected tweets.

UGC User generated content.

VPN Virtual Private Network.

Widget An app that allows you to access another app or content via a shortcut, such as the options on your smart phone.

Some definitions courtesy of University of Colorado,
social.colostate.edu/trends/25-social-media-terms- you-should-know-in-2021/

References

AndrewJ. (2022) "Top 17 OSINT tools to find anyone online 2022". *LinkedIn*. (April 10)

Arnaudo, D., B. Barrowman, J. Brothers, L. Reppell, V. Scott, A. Studdart, K. Wainscott, and V. Zakem (2021) *Countering Disinformation Guide*. Washington, DC: US AID and Consortium for Elections and Political Process Strengthening.

BBC News (2022a) "Cyber-security chiefs warn of malicious app risk" www.bbc.com/news/technology-613233954

BBC News (2022b) "74% of ransomware revenue goes to Russian hackers" www.bbc.com/news/topics/c1xp19421ezt/cyber-crime

Cobwebs (2022)) cobwebs.com/resource/case-study/digital-risk-protection/using-digital-risk- protection-platform-in-times-of-crises/)

Colorado State University (2021) Social Media Terms You Should Know in 2021 at social.colostate.edu/trends/25-social-media-terms-you-should-know-in-2021/

Congressional Research Service (2022) *Law Enforcement and Technology: Using Social Media* Washington, D.C.

- ----------(2021) *Social Media: Misinformation and Content Moderation Issues for Congress* Washington, D.C.

Degani, M. (2020) "Exploiting Social Media in Gang Cases" *DOJ Journal of Federal Law and Practice.*

Dreisbach, T. (2021) "How Extremists Weaponize Irony to Spread Hate" *National Public Radio,* April 26. www.npr.org/2021/04/26/990274685/how-extremists-weaponize-irony-to-spread-hate

Economist (2017). "Two of the biggest dark-web markets here have been shut down." (July 21)

Ekwunife, N. E. (2002) *National Security Through Social Media Intelligence Domestic Incident Prediction.* Marymount University dissertation.

Express VPN (2022) www.expressvpn.com/blog/best-onion-sites-on-dark-web/

Finkelstein, J., A. Goldenberg, S. Stevens, L. Jussim, J. Farmer, J. Donahue, and P. Paresky (2020) *Network-Enabled Anarchy: How Militant Anarcho-Socialist Networks Use Social Media to Instigate Widespread Violence Against Political Opponents and Law Enforcement*, Rutgers Miller Center for Community Protection and Resilience. New Brunswick, NJ.

Gips, M. and P. Goldenberg (2021) "Countering disinformation: An essential new role for CSOs" *Security Magazine* (October 27).

Global Justice Information Sharing Initiative and International Association of Law Enforcement Intelligence Analysts, Inc. (2012) *Law Enforcement Analytic Standards, 2nd Edition*. Washington, DC.

Global Web Index (2022) "Social Media Across Generations" at www.gwi.com/reports/social- media-across-generations

Government Accountability Office (GAO) (2022) *Federal Agencies' Use of Open-Source Data and Related Threat Products Prior to January 6, 2021*. Washington, DC. (May)

Hollywood, J., M. Vermeer, D. Woods, S. Goodison and B. Jackson (2018) *Using Social Media and Social Network Analysis in Law Enforcement*. Rand Corporation.

Horwitz, J. and D. Seetharaman (2020) "Facebook Executives Shut Down Efforts to Make the Site Less Divisive". *Wall Street Journal* (May 26).

Immigration and Customs Enforcement (2022) "IPR Center helps seize $11M in illicit medicines in global Interpol operation" https://www.ice.gov/news/releases/ipr-center-helps-seize-11m-illicit-medicines-global-interpol-operation

International Association of Chiefs of Police (2019) *Social Media Policy.* Alexandria, VA.

Investopedia (2022) "What is a Blockchain?" www.investopedia.com

Krippendorff, K. (1989) "Content Analysis" In E. Barnouw, G. Gebner, W. Schramm, T.K. Worth, & L. Gross (eds). *International encyclopedia of communication* (Vol 1.) New York, Oxford University Press.
Law Enforcement Social (2020) www.facebook.com/LEDotSocial

Maltego (2022) *Handbook for Social Media Investigations.* Maltego Technologies.

Marcellino, W., M. Smith, C. Paul, and L. Skrabala (2017) *Monitoring Social Media.* RAND Corporation, Santa Monica, CA.

Muhammad, A., Y. Ibrahim, A. Abubakar (2018) "Exploitation of Social Media for Open-Source Intelligence" in *Journal of Multi-Disciplinary Engineering Technologies*, Vol. 12, Issue 1.

Obar, J. and S. Wildman (2015) "Social media definition and the governance challenge: An introduction to the special issue". *Telecommunications policy*, 39 (9), 745-750.

Pennybacker, G. and K. White, (2021) "Focus on Social Media Effectively Managing Messages." FBI *Law Enforcement Bulletin* (LEB) Federal Bureau of Investigations, Washington, D.C. (February 11).

Pew Research Center (2021) "Social Media Fact Sheet". Washington, DC (April 7)

Spiliotopoulou, L., Y. Charalabidis, E. Loukis and V. Diamantopoulou (2014) "A framework for advanced social media exploitation in government for crowdsourcing" University of the Aegean and Research Gate.

Statistica (2022) www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

ThomsonReuters (2022). "Social Media in Law Enforcement Investigations."

Truelist.co (2022). truelist.co/blog/tor-stats/

U.S. Attorney's Office (2021) "Former Jacksonville Second Grade Teacher Pleads Guilty To Distributing Child Sexual Abuse Videos Using Social Media App" (August 24).

- ---------- (2018) "Nicholasville Men Sentenced for Social Media Threats Related to School Shooting Hoax" (September 28).

----------(2021) Two District Men Indicted for Violent Kidnapping Live-Streamed on Social Media (March 21)

U.S. Department of Justice (2018) "Use of Social Media to Communicate with the Public".

University of South Florida (USF) (2022). "Introduction to Social Media" at www.usf.edu/ucm/marketing/intro-social-media.aspx

Vaughan, L. (2005). "Social Network Analysis." *Encyclopedia of Social Measurement*. www.sciencedirect.com/topics/social-sciences/social-network-analysis

Wardle, C. and H. Derakhshan (2017) "Information Disorder: Toward an interdisciplinary framework for research and policy making". Council of Europe report DGI (2017)09.

Whitney, M . (2022) "39 Twitter Statistics Marketers Need to Know in 2022". Wordstream.com.

Yacub M. (2022) "How Many Tweets Per Day". *Smart Insights.* (June 7).

IALEIA

IALEIA is the largest professional organization in the world representing law enforcement analysts. It is based in the United States and is a nonprofit 501(c) 3 educational corporation. IALEIA is managed by an international Board of Directors consisting of eleven elected IALEIA members.

IALEIA supports regional chapters throughout the world. It represents law enforcement analysts in a variety of venues, and provides a community environment by establishing regional chapters

IALEIA has a certification program for analysts, a code of ethics, and bylaws that provide structure for the organization. It offers both basic and advanced analytic training and holds a yearly training conference along with the Association of Law Enforcement Intelligence Units (LEIU).

Members come together to achieve the following objectives:

- **Advocacy.** IALEIA unites members and advances public and official understanding of criminal intelligence analysis and its role as a profession. Members of the Board of Directors regularly represent IALEIA as subject matter experts at international and national meetings.
- **Training.** IALEIA devises concepts, standards, and curricula for training.
- **Certification.** IALEIA has qualification standards and indices of competence for the profession and administers a professional international certification program. The IALEIA Analyst Certification Program is structured to encourage continuing education, measure knowledge and skills, and recognize excellence though experience.
- **Networking.** Regular meetings, training, and speakers are arranged by the numerous regional IALEIA chapters worldwide. By providing timely, relevant information to members on opportunities and issues affecting the field, IALEIA promotes well-informed career analysts. In addition, IALEIA's website (www.ialeia.org) is available in several languages to facilitate international networking opportunities.
- **Professionalism.** The organization reinforces the concepts of professionalism, dedication to service, and integrity among practitioners of criminal intelligence analysis.
- **Research.** IALEIA encourages research about criminal intelligence analysis, the analytic process, and identifies funding for such research

For information on IALEIA membership, certification, Board Members, partnerships, training, and any other information, please visit www.ialeia.org.

IALEIA Corporate Members

Blue Light, LLC

Chorus Intelligence

Esri

First Alert Powered by Dataminr

Fivecast

GeoTime

i2 Group

International Anti-Crime Academy

Kineviz

Lexis Nexis Risk Solutions

Montel Technologies

Ntrepid

PenLink

Pipl

VA Analytics