ADVANCED INVESTIGATIVE TACTICS

GEORGE FLORES

ACCOUNT MANAGER

GFLORES@DIGISTREAM.COM

510-871-7686

WHAT IS OSINT? WHAT IS SOCMINT?

According to the FBI, open-source intelligence "refers to a broad array of information and sources that are generally available, including information obtained from media (newspapers, radio, television, etc.), professional and academic records (papers, conferences, professional associations, etc.), and public data (government reports, demographics, hearings, speeches, etc.)."[1]

According to AFIO's The Intelligencer, open-source intelligence "is defined as the collection, processing, analysis, production, classification, and dissemination of information derived from sources and by means openly available to and legally accessible and employable by the public in response to official national security requirements."[2]

DEFINITION AND SCOPE OF "SOCIAL MEDIA INTELLIGENCE"

Social media intelligence (SOCMINT) is an intelligence discipline built upon tools and solutions for social media monitoring. This methodology is able to apply intelligence tools to efficiently analyze a wealth of information hidden in social networks to detect early signals of important events, get a picture of public sentiment on target topics, monitor trends, identify influencers, and extract actionable intelligence to assist decision support.[3] Social media intelligence allows one to collect information from social media sites using both intrusive and non-intrusive means from open and closed social networks.

CURSORY ONLINE SEARCH STRINGS

Begin with direct queries of top 4 social media sites Facebook, Instagram, Twitter, YouTube then move to following Google/Yahoo/Bing searches:

- "John Smith" + New York, NY
- "Smith, John" + New York, NY
- "John Smith" + [known hobby/interest]
- "unicorn20@gmail.com"
- "unicorn20"
- inurl: unicorn20
- "510.555.1234

[1] "Intelligence Branch." *FBI*. FBI, 03 May 2016. Web. 02 Dec. 2016., https://www.fbi.gov/about/leadership-and-structure/intelligence-branch

[2] "Old Intelligencer." *The Mathematical Intelligencer* 6.4 (1984): 71-78. AFIO. Web., https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf

[3] "Social Media Intelligence SOCMINT 2016." *SOCMINT*. N.p., n.d. Web. 02 Dec. 2016., http://www.socmint.org/

COMMON ONLINE INVESTIGATIVE CHALLENGES

Identity Resolution

"And how did you verify that this account that hadn't been used in years was Mr. Smith?"

- Full Name
- Geographic indicators (photos of residence)
- Email address
- Known handle
- Friends with confirmed relatives
- City of residence
- Self-reference
- Birthday
- Photographic

Chronological Resolution

"So you have no way of knowing that's when it was posted or that's when it was last accessed, correct?" or *"Can you tell me the date the photo was actually taken, not when it was uploaded online?"*

- Captions and comment threads verifying capture date
- OSINT (Open Source Intelligence) methodology
    - Race/event results
    - League/team rosters and schedules (athletes)
    - Performance venue schedules (Concerts, comedians)
    - Event agendas (galas, conferences, etc.)
- Ask plaintiff/claimant to produce content on native device in native format to confirm capture date

Preservation

- Electronic Vault (E-Vault)
- Bibliography (live URL, Identity Resolution metrics

Authentication / Metadata

The following are some key metadata fields for individual Facebook posts (such as a photo or status update) that together provide important information to establish authenticity of online activity, if properly collected and preserved:

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

Best Online Investigative Practices

- Background check (Criminal, Civil, Property)
- Content collection
- Identity resolution
- Preservation
- Analysis
- Authentication (Metadata)
- Account monitoring
- Testimony

Current OSINT Community: Recent Trends

LIVESTREAMING

(Facebook Live, Periscope): live video of an event or discussion (uploading in real-time). Mark Zuckerberg announced this new feature for Facebook (for all users) in a 6 APRIL 2016 status update.

- People spend 3x more time watching a Facebook Live video on average compared to a video that's no longer live. This is because Facebook Live videos are more interesting in the moment than after the fact[4].
- Expected growth with increased video quality, mobile phone viewing capabilities, decline of Traditional Television watching methods.
- Periscope is a live video streaming app for iOS and Android that was acquired in March 2015 by Twitter and relaunched

[4] "News Feed FYI: Taking into Account Live Video When Ranking Feed | Facebook Newsroom." *Facebook Newsroom*. N.p., n.d. Web. 02 Dec. 2016. http://newsroom.fb.com/news/2016/03/news-feed-fyi-taking-into-account-live-video-when-ranking-feed/

GEOTAGGING

electronic tag assigns a geographical location to a photograph or video, a posting on a social media website, etc. based on latitude and longitude coordinates. Clicking on the geotag in Twitter and Instagram shows you other posts that use that geotag.

- Location based SMS (text messages) introduced in 2007 - applications capable of displaying locations on GoogleMaps.[5]
- Because of the requirement for wireless service providers in United States to supply more precise location information for 911 calls by 11 SEP 2012 more and more cell phones have built-in GPS chips.
- Later introduced to social media platforms, Facebook, Twitter, Instagram
- Study done by JiWire suggests that 62% of social media users include location tags in posts on different platforms that included Facebook, Instagram, Twitter and Google+. The majority of respondents (49%) use location tags to let their friends and family know where they're shopping and traveling. Facebook: 91% of respondents use the platform on the go and 88% tag their locations at least monthly[6].

"FRIENDING": LEGALITY, PRACTICALITY, AND ETHICS[7],[8]

US V GATSON & FACEBOOK RESPONSE

- Bergen County police department sent request to be friends without a warrant with Gatson on his Instagram account, which included photos of items that Gatson had stolen. Gatson accepted the request and law enforcement was able to view all content on the account. Conclusions reached for this case included:
    - "No search warrant is required for the consensual sharing of this type of information."
    - "Gatson's motion to suppress the evidence obtained through the undercover account will be denied."
- In response, social media sites started "notifying account holders when their data is requested by law enforcement." Facebook also requires a "valid subpoena, court order or search warrant" if law enforcement wants to search Facebook for records.

---

[5] "A History of SMS Geotagging." *GeoSMS*. N.p., 17 Oct. 2010. Web. 02 Dec. 2016. https://geosms.wordpress.com/2010/10/18/a-history-of-sms-geotagging/

[6] Griwert, Katherine. "Rise of Geotagging Points to Need for Local Social Marketing." *Brafton*. N.p., 29 Aug. 2012. Web. 02 Dec. 2016. http://www.brafton.com/news/rise-of-geotagging-points-to-need-for-local-social-marketing/

[7] Muse, Seth. "Advertisement." *Ethics of Using Social Media During Case Investigation and Discovery | ABA Section of Litigation*. American Bar Association, 13 June 2012. Web. 02 Dec. 2016. http://apps.americanbar.org/litigation/committees/pretrial/email/spring2012/spring2012-0612-ethics-using-social-media-during-case-investigation-discovery.html

[8] Lawyers, The National Trial. "LawyersandSettlements.com." *Lawsuits, Legal News & Issues, Lawsuit Settlements, Class Action Lawsuits*. N.p., 05 Feb. 2015. Web. 02 Dec. 2016. https://www.lawyersandsettlements.com/articles/internet-technology/fake-social-media-account-20433.html

STORED COMMUNICATIONS ACT[9]

- apply to the "reasonable expectation of privacy" in an online context. Users generally entrust the security of online information to a third party, an ISP. In many cases, Fourth Amendment doctrine has held that, in so doing, users relinquish any expectation of privacy. The Third-Party Doctrine holds "that knowingly revealing information to a third party relinquishes Fourth Amendment protection in that information."

FEDERAL RULE OF EVIDENCE 902(11)(12)

- Federal Rule of Evidence 902(11) states, "The original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)-(C), as shown by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court. Before the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record — and must make the record and certification available for inspection — so that the party has a fair opportunity to challenge them."

- Federal Rule of Evidence 902(12) states, "In a civil case, the original or a copy of a foreign record that meets the requirements of Rule 902(11), modified as follows: the certification, rather than complying with a federal statute or Supreme Court rule, must be signed in a manner that, if falsely made, would subject the maker to a criminal penalty in the country where the certification is signed. The proponent must also meet the notice requirements of Rule 902(11)."

Federal Rule of Evidence 902(11)(12) state you do not need an investigator who conducted an online investigation to physically testify in court as affidavits detailing the mechanisms of the investigation are considered legitimate substitutes to witnesses. Rule 803(6)(A)-(C) essentially designates a regularly conducted business activity, i.e. an investigation, being documented by the individual who engaged in said activity as a qualified witness and the featured rules permit that documentation to be presented in lieu of a person.

ABA FORMAL OPINION 466

Released 24 APRIL 2014, Formal Opinion 466 states, "There is a strong public interest in identifying jurors who might be tainted by improper bias or prejudice. There is a related and equally strong public policy in preventing jurors from being approached ex parte by the parties to the case or their agents. Lawyers need to know where the line should be drawn between properly investigating jurors and improperly communicating with them."

"Passive review of a juror's website or ESM, that is available without making an access request, and of which the juror is unaware, does not violate Rule 3.5(b). In the world outside of the Internet, a lawyer or another, acting on the lawyer's behalf, would not be engaging in an improper ex parte contact with a prospective juror by driving down the street where the prospective juror lives to observe the environs in order to glean publicly available information that could inform the lawyer's jury-selection decisions. The mere act of observing that which is open to the public would not constitute a communicative act that violates Rule 3.5(b)."

---

[9] "18 U.S. Code Chapter 121 - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS." *LII / Legal Information Institute*. N.p., n.d. Web. 02 Dec. 2016. https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121

SAMPLE DEFENDANTS' SOCIAL MEDIA INTERROGATORIES TO PLAINTIFF

Please identify all of your internet social media and networking websites and/or applications, which you have used and/or maintained an account in the last six (6) years. Internet social media websites include, but are not limited to, Facebook, LinkedIn, Twitter, Instagram, Foursquare, YouTube, Pinterest, Google+, Tumblr, Flicker, Skype, FaceTime, etc.

1. For each internet social media website account, please provide your username and password, or alternatively, under Rule 1.34(c), please provide a copy of all non-privileged content/data shared on the account(s) in the last six (6) years. In the event you contend there is a privilege to assert, please provide a privilege log.

2. Please identify any and all photograph, still image, and video sharing websites that you have used and/or maintain(ed) an account in the last six (6) years. "Internet photo, still image, or video sharing website" is defined as websites in which a user can upload/post/ view still or video image content, which is hosted for and shared public use, which includes but is not limited to YouTube, Shutterfly, Tumblr, Photobucket, Vine, Instagram, etc.

3. For internet photo, still image and video sharing website accounts, please provide your username and password, or alternatively, under Rule 1.340(c), please provide a copy of all non-privileged content/data shared on the account in the last six (6) years. In the event you contend there is a privilege to assert, please provide a privilege log.

4. Please identify any and all blog or internet message boards, chat rooms, and public forums that you have participated in or a member of within the last six (6) years. "Internet message board or public forum" includes but is not limited to any internet website or service in which users post messages or content in a public-forum.

5. For each blog or internet message board, chat room, and public forum, please provide your username and password, or alternatively, under Rule 1.340(c), please provide a copy of all non-privileged content/data shared on the account in the last six (6) years. In the event you contend there is a privilege to assert, please provide a privilege log.

6. Please provide the name of any email account(s), which you have used and/or maintained in the last 6 years.

7. For any account identified in answer to Nos. 1 – 7, please describe in detail any and all content that you have deleted or erased on or after (insert date), including but not limited to photographs, videos, posts, tweets, and name/username chan

Agriculture's Common Issues When Confirming an Address for Surveillance

- The claimant might provide an address but is not living there.
- Claimant lives at the address but could be spending their time at their significant other's residence.
- Multiple individuals that are living in the same residence that have similar identifiers.

- The claimant might just provide a PO BOX as their address.

- The claimant may not have a personal vehicle; therefore, validating vehicle registration would not be fruitful.
- The claimant could be using an unidentified individual's vehicle.

- The claimant lives in a rural area making the ideal surveillance set-up challenging.

- The claimant may not have any state or federal documentation such as, but not limited to, an I.D., Driver's License, and Social Security Card.

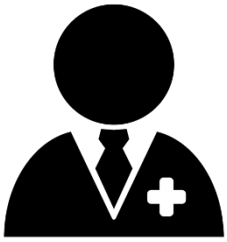
DigiStream INVESTIGATIONS

Agriculture's Best Practices for Confirming an Address for Surveillance

- Utilize background records to determine all previous addresses associated with the claimant.
- Also, review all associates linked with the claimant, such as family members, friends, and old roommates, to determine where they might be living.

- If a PO BOX is provided, ask for a physical address for payroll purposes and have the claimant pick up their check at the Human Resource office.

- Emergency contacts can be a great source for initiating investigations for two reasons:
  1. Cross-referencing their addresses with the claimant's; Are they sharing the same address?
  2. Claimant provides a PO BOX as their address, look into their emergency contacts. They can play a vital role in initiating the investigations.



- QME (Qualified Medical Evaluators)
- Medical Appointment:
  a. Follow up visits with their doctor
  b. Physical Therapy

- Legal Deposition

REASONS TO INTERVENE EARLY IN A CLAIM

OVERVIEW

It is important to take an aggressive stance in protecting your organization from false claims. When claimants take advantage of the system and know their employer will cover the claim with no questions asked, claims tend to go on the rise. Proactively creating protocols to combat suspicious claims early saves time and money and protects the company's best interest. For example, if intervention occurs early enough, the subject may not yet be represented, making it easier to access them for an interview or informal conversation. Moreover, experience has proven that represented subjects are often made aware of the potential for surveillance. Early intervention allows the investigative firm to operate more freely, with the claimant unaware of the investigative resources available to the insured.

BACKGROUND CHECK

Identifying the root cause of motivations behind misrepresenting the details of a loss is an essential aspect of an investigation. First, in states which provide an avenue for apportionment, knowledge of the subject's previous injuries may provide the insured an opportunity for cost containment. In addition, understanding the motivations behind claim abuse can help shape an investigative strategy. Such motivations may include financial distress leading to outside employment, starting one's own business, a history of successful litigation, or a lack of personal health insurance among a host of others.

SOCIAL MEDIA

The earlier the investigation, the greater the chances of uncovering actionable content from the claimant's social media. This is helpful if the claimant is instructed to remove or hide content. When notable social media content is found, it is critical to preserve it immediately. Social media, a valuable compliment to surveillance, not only captures what is happening that day but also documents information from the past, present, and future. At DigiStream, we see a 43% increase in surveillance video when the assignment is coupled with a social media investigation.

SURVEILLANCE

Surveillance has been the cornerstone of the claims investigation industry for decades. When a claimant is surveilled immediately after a loss, the claimant is often not represented and not aware of the potential for surveillance. Moreover, if surveillance is conducted early enough, that evidence can be provided to a physician prior to an appointment, increasing the chances of the subject returning to work. While the industry has evolved considerably with the introduction of social media, surveillance remains the best avenue to refute a claimant's self-reported limitations.

DigiStream® INVESTIGATIONS

DigiStream INVESTIGATIONS

10 MOST COMMON CLAIMS

WORKER'S COMPENSATION AND GENERAL LIABILITY RED FLAGS

Red Flag	Description	DigiStream Solution
Monday Morning Injury	Loss / injury occurs at the start of a shift immediately following a day off, or immediately upon arriving on premises of Insured.	**SocialPRO® MED**
Employment Just Began or About to End	Employee was just hired, is disgruntled, soon-to-retire, or facing imminent firing or layoff.	**SocialPRO® PLUS Surveillance**
Financial or Personal Hardship	Claimant is experiencing financial difficulties and/or domestic problems prior to submission of claim.	**SocialPRO® PLUS**
Doctor Shopping	Claimant changes physician when a release for work has been issued, or a diagnosis inconsistent with injuries.	**Medical Sweep PhysicianView™**
Late Reporting	First notification of injury or claim is made after employee is terminated or laid off. Notification of GL claim occurs weeks, months or years after alleged loss.	**SocialPRO® PLUS Surveillance**
Outside Employment	"Tip" indicates that the totally disabled worker is currently employed elsewhere	**SocialPRO® PLUS Surveillance**
Claimant is Never Home	After filing a claim, claimant is never home or spouse/relative answering phone states the claimant "just stepped out," or may have to contact him/her by pager.	**SocialPRO® PLUS Surveillance**
Frequent Appointment Cancelations	Claimant cancels or fails to keep appointments.	**Recorded Statement SocialPRO® PLUS**
No Witnesses	Accident is not witnessed, or witnesses to the accident conflict with the claimant's version or with one another.	**Recorded Statement GeoSocial Sweep™**
Recurring Injury	Alleged injury relates to a pre-existing injury or health problem	**Medical / Pharmacy Sweep**