News, Resources and Useful Information for the Online Investigative and OSINT Professional from Toddington International Inc.

Toddington International Inc.

Online Research and Intelligence Newsletter

APRIL 2019 EDITION

In This Edition

Welcome to the Newsletter

Welcome to the April 2019 edition of the newsletter.

We just finished up the first Vancouver- and Toronto-based installments of our "*Advanced Internet Intelligence & Online Investigations*" training for the year and would like to thank our delegates who traveled from as far as the UK to attend. We will have new dates scheduled for the Fall 2019 installments soon. Contact us to join the course wait list.

We are back in Vancouver and Toronto for our "*Social Media Intelligence & Online Investigations*" training in May and June, and look forwarding to seeing you there.

Our featured article this month provides an overview of Social Media Intelligence (SOCMINT). We explain what it is and why it is essential for investigators and researchers in every capacity. Critical sources of social media intelligence, or social media platforms, will be presented, in addition to legal considerations for investigators.

Also in this newsletter, we share our monthly round-up of online investigative and security tools, and our favourite industry-related articles that our team has found to be of particular interest.

E-Learning Graduates

Congratulations to the following students who are among the latest to have successfully completed the 40-hour Using the Internet as an Investigative Research Tool™ e-learning program with TII:

- Jolayemi Akerele
- Julie Norman
- Cameron Boyle
- Peter Kovacec
- Michelle Hunt
- Juanita Gaber
- Debdulal Karmaker
- Tarah Vallee
- Scarlett Kelly
- Eric Larsen
- Donat M'Baya Tshimanga
- Theresa Moore
- Paige Newman

Important Note: As we respect the privacy of our students, we only publish the names of students who have provided express permission to do so. Many of our students are unable to share their completion due to the nature of their employment, or due to online privacy concerns. If your name did not appear in the above list and you wish to announce your completion of the course with TII, please contact us.

Social Media Intelligence: An Overview

What Is Social Media?

commentary, in addition to interests, opinions, groups, "likes," and multi-media, including images and videos. For investigative and research professionals, social media is a rich source of intelligence that should always be leveraged.

What Is Social Media Intelligence?

Social Media Intelligence (otherwise known as "SOCMINT") is processed information, sourced from online social platforms and applications that facilitate and enable the collecting, monitoring, and analysis of up-to-date online sentiment and social commentary. The rich and varied information available from social platforms may be live or historical, opinion or fact, text or multi-media, proprietary or crowd-sourced; depending on the data provided by each source, and an investigator's ability to cross-reference the data across platforms and tools, a comprehensive profile of an individual, location, or event can often be built quickly and accurately.

What Types of Social Media Platforms Can Investigators Leverage for Intelligence?

When we think of social media, what immediately comes to mind are the most familiar social platforms: Facebook, Twitter, Instagram, and LinkedIn. However, social media encompasses various categories of content that are often not considered when we think of this source of information, including:

Multi-media sharing:

- YouTube (videos)
- Tumblr (images, videos)
- Flickr (images, videos)
- Pinterest (images)
- DeviantArt (images, videos)
- Myspace (images, videos, music)
- Vimeo (videos)
- TikTok (videos)
- Twitch (live video streaming)
- Vine (videos) vine.co/[username] (no longer available, but archived videos can be viewed by entering a username after the forward-slash in the URL)

Chat-based or instant-messaging applications (many of which incorporate image- and video-sharing):

- WhatsApp
- Snapchat
- Skype
- Viber

- Reddit
- Digg
- Pinterest
- Mix

Ratings-based:

- Trip Advisor
- Yelp

Location-based:

- Foursquare

Blogging:

- WordPress
- Google Blogger
- LiveJournal

Discussion forums:

- Google Groups

Region-specific:

- VK (Russia)
- OK or Odnoklassniki (Russia)
- QQ (China)
- Sina Weibo (China)
- WeChat (China)
- QZone (China)
- TikTok (China)
- Xing (Europe)

There are many more social media and networking sites and/or applications available than what is listed above, as well as additional categories. Investigators should (at the very least) know of the different social platforms that are available and most popular in their region of interest; a subject's location should always be considered when developing a social media research plan. If a subject is based in Russia or China, for example, he or she may not be found on platforms that are popular in North America.

What Information or Intelligence Can Be Leveraged from Social Platforms?

A great deal of information can be gathered about a subject or individual from

coordinates) from meta data, an individual can be placed at a given location, on a given date, at a given time. By viewing a social media user's network of contacts, relationship information can be gathered, associates (secondary subjects) can be located, and business activities can be revealed. Moreover, from an individual's profile and shared content, an investigator can learn of their interests, daily activities, sentiment or opinions regarding different topics, and even reputation; with such varied information about a subject, much of it coming from the subject directly, a comprehensive profile can be constructed.

SOCMINT plays an increasingly critical role in proactive and reactive police operations at all levels. However, it is not only reserved for law enforcement activities — it can benefit investigators and researchers in every capacity. For insurance and fraud investigators, SOCMINT can provide insight into the lifestyle and activities of a subject, sometimes providing digital evidence for litigation; for financial professionals, it can assist "KYC" practices; for human resource managers (or managers and employers in general), it can aid in background-checking; for corporations and businesses, it can provide competitive intelligence; for private investigators, it can be used to conduct reconnaissance for planned surveillance; for journalists and researchers, it is an endless gateway to global research sources.

How Many Social Media Users Are There and How Much Content Do They Contribute?

Social media users make an exhaustive amount of contributions to the prolific content that is shared on these platforms; the number of social media users continues to increase, as does the amount of social content that is shared. Facebook alone has over two billion active users; Instagram has one billion users; Twitter has over 300 million users; and LinkedIn has over 500 million users. More staggering than the number of social media users is the amount of information that is shared on social platforms. On a daily basis, Twitter sees an estimated 500 million tweets; approximately 350 million photos are uploaded to Facebook; Instagram users post just under 100 million posts, in addition to 500 million "stories"; Snapchat users post over 3 billion snaps; over 60 billion messages are sent via WhatsApp; and approximately 300 hours of video are uploaded to YouTube. This is the amount of social data generated every single day, and does not even include all of the social media platforms that are available.

What Is Social Media Monitoring?

Social Media Monitoring is the process of tracking social content on various different channels through the use of specialized tools. Essentially, these tools "listen" to what is being said or shared online. With the overwhelming amount of content that is shared on social media every day, investigators and researchers

including:

- HootSuite
- Social Mention
- TweetDeck
- FollowerWonk

Furthermore, when monitoring a specific subject, location, or event, investigators may want to consider real-time, geo-location based social media discovery or monitoring platforms, such as those listed below. Location-based discovery platforms allow users to select a location of interest, or search for locations a subject has posted from; some platforms even allow users to set up a "fence" surrounding an area of interest to retrieve social media posts made from the location. The better platforms allow for automation, enabling users to set up "alerts" as to when a subject posts, or when posts are made from a given location; these automated tools often allow for results to be filtered by keyword, location, and/or user to prevent information overload.

- Echosec
- Snaptrends
- Google Alerts
- Tweepsmap
- Trendsmap
- Worldcam
- Twitterfall
- Awario
- Sprout Social

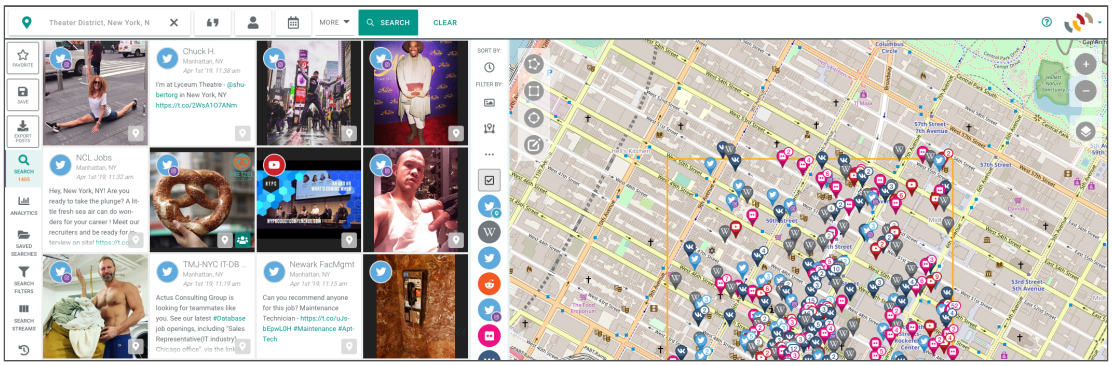

Image Source: Echosec.net

What Are Legal Considerations When Leveraging Intelligence Gathered from Social Platforms?

By its very nature, social media is a double-edged sword. On the one hand, it is a treasure trove of intelligence, very often providing valuable insight to progress investigations via new avenues of discovery through information shared by subjects and their associates. On the other hand, it introduces a very important

the circumstances in which such evidence is gathered.

Many factors will be considered by the courts when assessing the admissibility of electronic evidence, including the manner in which it was obtained. Investigators should always consider: What is this user's expectation of privacy? Is the account private, or viewable by the general public? Were deceptive tactics employed in gathering the evidence?

It should be understood that electronic evidence gathered from social media platforms cannot be retrieved in a deceptive manner; investigators should not go and "friend" their subjects in an attempt to gather information. Moreover, in order to be admissible in most legal systems, electronic evidence must also be relevant, reliable, and authentic. For example, was the image an original image, or was it somehow photo-shopped? Was it actually the subject that posted the post in question, or was his or her account hacked or otherwise compromised?

Each country, jurisdiction, and organization will have their own legislation and guidelines governing the use of social media (or electronic information) for evidentiary purposes. It is the investigator's responsibility to become familiar with case law and legislation governing the admissibility of electronic evidence in their country or jurisdiction. For criminal investigations, the prosecutor — whether it is the Crown Counsel (in Canada), the Crown Prosecutor (in the UK), or the District Attorney (in the US) — should be an investigator's best friend. When in doubt, investigators should err on the side of caution and first consult legislation and case law, or the jurisdiction's presiding prosecutor.

To learn more about leveraging the value of social platform-sourced intelligence for research or investigative purposes, in a manner that does not violate user privacy expectations or other legal limitations, join us on our "*Social Media Intelligence & Investigations*" training in Vancouver, BC, on May 16-17, or in Toronto, ON on June 6-7.

Upcoming Select Public Courses

Social Media Intelligence & Investigations

To recognize, collect, and leverage the value of social platform-sourced information, research and investigative professionals must fully understand the restrictions and implications of obtaining and utilizing such information in a manner that does not violate user privacy expectations, license agreements, and other legal limitations. This course will introduce research and investigative professionals to a variety of innovative tools and techniques that will enable you to locate, collect, and utilize social platform-sourced information, while considering the implications of leveraging this type of information safely, quickly, and appropriately.

May 16-17, 2019, Vancouver, BC*

June 6-7, 2019, Toronto, ON*

**Only a limited number of seats are available at the early-bird rate, based on a first come, first served basis. Sign up early to receive the discounted pricing.*

Advanced Internet Intelligence & Online Investigations

Aimed at managers, frontline investigators, researchers, and analysts alike, this advanced training program will provide detailed instruction on effectively using the Internet as an Open Source Intelligence, research, and investigation tool. Demonstrating advanced search and analysis techniques for mining Web-based and social media information, this comprehensive training program will also examine a number of essential privacy tools for ensuring data, communication, and online security. Techniques being used by the criminal element to conceal their identity, location, and illegal behaviour will also be introduced.

September 8-11, 2019, Cambridge, UK

Australia- & Asia-Based Training

We will also be in Australia, Hong Kong, and Singapore for training in the upcoming months. For dates, locations, and pricing information, please contact us.

TII is pleased to offer a number of specialized and customizable in-house training programs for both the public and private sector in a variety of formats. We also have available a number of expert speakers available. To learn more about what we can do to empower your workforce, contact us.

Resources for the OSINT Professional

https://mewe.com – An alternative to Instagram and Facebook, with a more privacy-focused approach, free from tracking, spying, and scraping

https://www.mp4joiner.org – Free software for manipulating MP4 files, including splitting and merging videos

http://socialmention.com – Real-time social media search engine

http://boardreader.com – Search engine for forums and message boards, with advanced search features available

https://mentionmapp.com – Twitter network mapping/visualization tool

https://metager.org – Meta search tool that searches over 50 search engines anonymously through a proxy and the 'Hidden-Tor-Branch'

https://www.eff.org/https-everywhere – Browser extension for Firefox, Chrome, and Opera that encrypts visits to websites for more secure browsing

https://breachalarm.com – Check to see if your email address has been compromised in a security breach

https://www.startpage.com – Searches Google privately by removing all trackers and logs, and blocks advertisements

https://panopticlick.eff.org – Test if your browser is safe from tracking, or whether it is leaking identifiable information

Intelligence Resources page to see more resources like these.

More Online Training

Open Source Intelligence for Financial Investigators
40-Hour E-Learning Program

Essential for all financial institutions and corporations required to comply with the *European Union Fourth Anti-Money Laundering (AML) Directive* and similar legislation, or otherwise engaging in enhanced due diligence activities, this comprehensive training provides financial and business professionals with the latest tools and techniques required to effectively gather online OSINT, with the aim of enhancing compliance activities and minimizing potentially detrimental risks to an organization — both quickly and accurately. **Sign up or learn more** here.

This course has been brought up multiple times by a few people I have come across in the financial crime industry for a good reason. From the very beginning when I was inquiring about the program, [TII's representative] responded to my questions quickly and thoroughly, leaving me feeling confident about taking the program. Unlike other courses that are only filled with PowerPoint slides full of information, this course focuses on real world application. You are applying the new skills that you learned while progressing through the modules which makes it easier to grasp the purpose of the lesson. The assignments for the modules were challenging and fair. Any questions that I had were clarified quickly by [the Instructor], and he provided assistance when I asked. I have learned so much through this course and I am confident that I will refer back to these skills as I progress in my career. – Balrob Randhawa (recent course graduate)

Introduction to Intelligence Analysis
40-Hour E-Learning Program

This program provides a rich and interesting opportunity to explore the key concepts and intellectual foundations which inform intelligence analysis activity. Students will develop awareness of, and experience in, using common tools and methodologies to conduct analysis assignments, as well as learn how to fashion one's insights and ideas in a way that communicates effectively to clients and other intelligence consumers. **Sign up or learn more** here.

Criminal Intelligence Analysis

This program is designed to equip aspiring and inexperienced analysts, as well as other interested law enforcement and investigative professionals, with the knowledge and skills required to undertake criminal intelligence analysis work, and to understand criminal intelligence analysis products when encountered. **Sign up or learn more** here.

Strategic Intelligence Analysis
40-Hour E-Learning Program

This program is intended for professionals working in public sector enforcement, intelligence, national security, and regulatory compliance roles, or those aspiring to do so. Students will be equipped with the skills and knowledge required to effectively conceive, plan, and implement strategic analysis projects, and deliver impactful strategic advice to clients and other end users. **Sign up or learn more** here.

"How-Tos" and Articles of Interest for the OSINT Professional

"Now Facebook is allowing anyone to look you up using your security phone number"

"How to Use Boolean Search for Social Media Monitoring (and Why You Want to)"

"10 Quick Firefox Tweaks to Maximize Your Online Privacy"

"How social media devastated two local restaurants"

"Internet Archive races to preserve public Google+ posts"

"Fifty years of the internet: What we learned, and where will we go next?"

"The paranoid person's guide to online privacy"

"The Internet Knows You Better Than Your Spouse Does"

"Here's what 25 popular websites used to look like back in the day"

"How the Internet Travels Across Oceans"

"Facebook's CEO Promises A More Privacy-Focused Future"

"Malware prevention and removal guide: How to remove malware and the best free tools to use"

"Facebook to launch its Clear History tool later this year -- to the joy of privacy advocates and the pain of advertisers"

"Why the Life-Insurance Industry Wants to Creep on Your Instagram"

"How to catch a catfisher"

"Facebook Privacy Settings: A Quick & Easy Guide for 2019"

"Russia bans smartphones for soldiers over social media fears"

"Password managers have a security flaw. But you should still use one"

"New AI fake text generator may be too dangerous to release, say creators"

Follow us on Twitter for daily articles and other interesting industry updates.

Copyright © 2019 Toddington International Inc., All rights reserved.