Social Media and Online Fraud Investigations

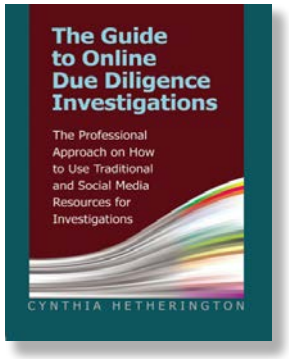
Rachel Kronenfeld

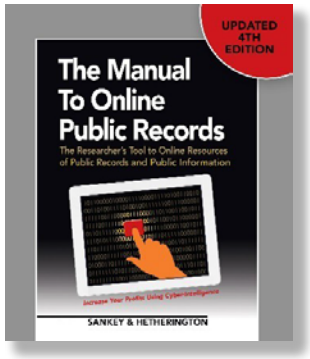
HetheringtonGroup

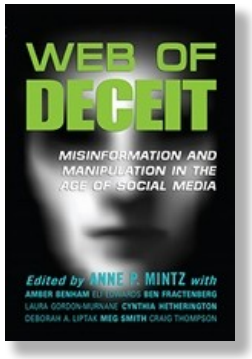
About Hg

- OSMOSIS Conference Host
- Publisher of data2know.com
- Authors
- Bloggers
- Investigators
- Analysts
- Trainers

OSMOSIS 2019 CONFERENCE







internet and online intelligence newsletter

data2know.com

A Publication of Hetherington Group

Overview

- Social media can be used to commit fraud.
- Social media can also be used to detect fraud.
- Potential incriminating evidence discovered through social media is increasingly being presented in court.

Scenarios

- Money laundering
- Identity theft
- Cyberstalking
- Cyberbullying
- Extortion
- Counterfeiting
- Corporate fraud
- Insider trading
- Insurance fraud
- Intellectual property theft
- Securities fraud
- Ponzi and pyramid schemes

Social media content

- Photographs
- Videos
- Live streams
- Status post
- Check ins
- Comments or replies
- Likes
- Shares

Beyond the content - analytics

- Geo-location data
- EXif data or metadata in photos and videos
- Account data-ID numbers, creation date
- Date posted
- Time posted
- Keywords used
- Social network (friends, followers)
- Conversations between users
- Connections between users
- Other link analysis

Privacy

- While a subject's account may be private, content may still be publicly accessible through their network of family and friends who may not have private profiles.
- A subject may think their profile is private. However, they may not have made all settings private, leaving some information still accessible.
- Consider that social media companies, particularly the larger ones such as Facebook, Instagram, YouTube and Twitter, will work with law enforcement to view protected information. Sometimes without a subpoena.

Consider tags and mentions

- Tagged photos, status posts and check ins
- Public posts or photos they have liked
- Public posts or photos by others they have commented on
- Public social media groups they are a member of
- Public friends or followers of others, to confirm connection to the subject

Deletion

- Deleted accounts may still live in website archives, and can sometimes be retrieved by law enforcement or with a subpoena.
- Deleted accounts may still leave behind content. For example, on Twitter if a profile was deleted, a searcher can still see conversations where the account was tagged or mentioned.
- Deleted photos, posts etc. may still be accessible through third party websites or archives.
- Forensic examination of the media involved will always

Prep for social media investigation

- Ask subject about their social media presence.
- Request subject provide all social media accounts.
- Have subject provide all aliases and usernames.
- Seek information on suspended or deleted accounts from the subject.
- Consider that your subject may not be truthful in giving up all information and accounts. -Investigation needed
- Or perhaps, the subject has simply forgotten about accounts if they are dated and have not been used in some time. -Investigation needed

Social media investigations

- Establish a plan
  - What are your expectations and goals?
  - Is there a particular social media platform of interest?
  - Is there a specific timeframe of interest?
  - Do you need a data dump? Capture of all content
  - Or do you need an analysis to look for something in particular?
  - Maybe both data dump and analysis.

Making the capture

- Common mistakes when capturing content, which may be not admissible as evidence in court.
  - No chain of evidence established
  - Image is not clear
  - Missing who posted the content
  - Missing where the content was posted from-URL if accessible
  - Missing when the content was posted- date and time stamp

Facebook

- Tip: To jump to particular years of a profile, start scrolling and look for this bar. Change recent to the year

- Tool: Facebook graph searching- the public information Facebook does not let you see. Using several tools, can locate public posts and photos subject is tagged in, liked or commented on by the subject and more.

Twitter

- Tip: Twitter advanced search (twitter.com/search-advanced)

- Tool: Tweetbeaver.com has several useful features. You can download a user's timeline, search within that timeline for a keyword and check if two accounts follow each other. You can also see what type of devise a user posted from and if they were using geo-location. Tweetbeaver.com includes only public information.

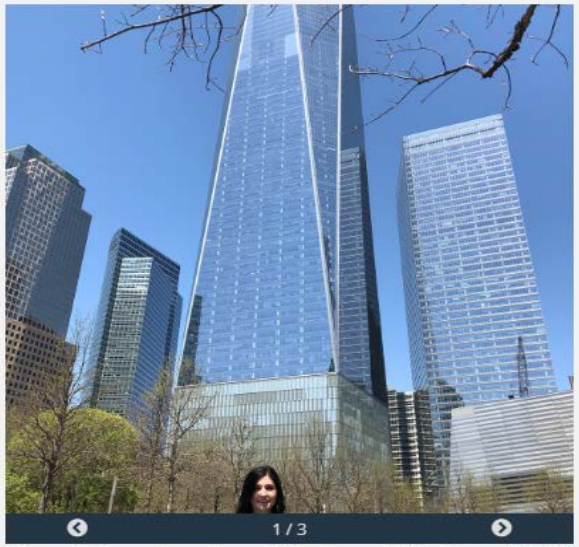
Instagram

- Tip: Remember to search hashtags and tagged photos

- Tools: Fee based tools such as Echosec, LifeRaftNavigator can keyword search public content, determine location of public posts if individual has geo-location turned on.

LifeRaft Navigator

Hetherington Group - Data2know
hetheringtongroup
Tue, May 1 2018, 5:49:44 pm EDT
New York, NY
Tags



Client visit on Broadway. #fearlessgirl #re2pect #911memorial

Meta Data

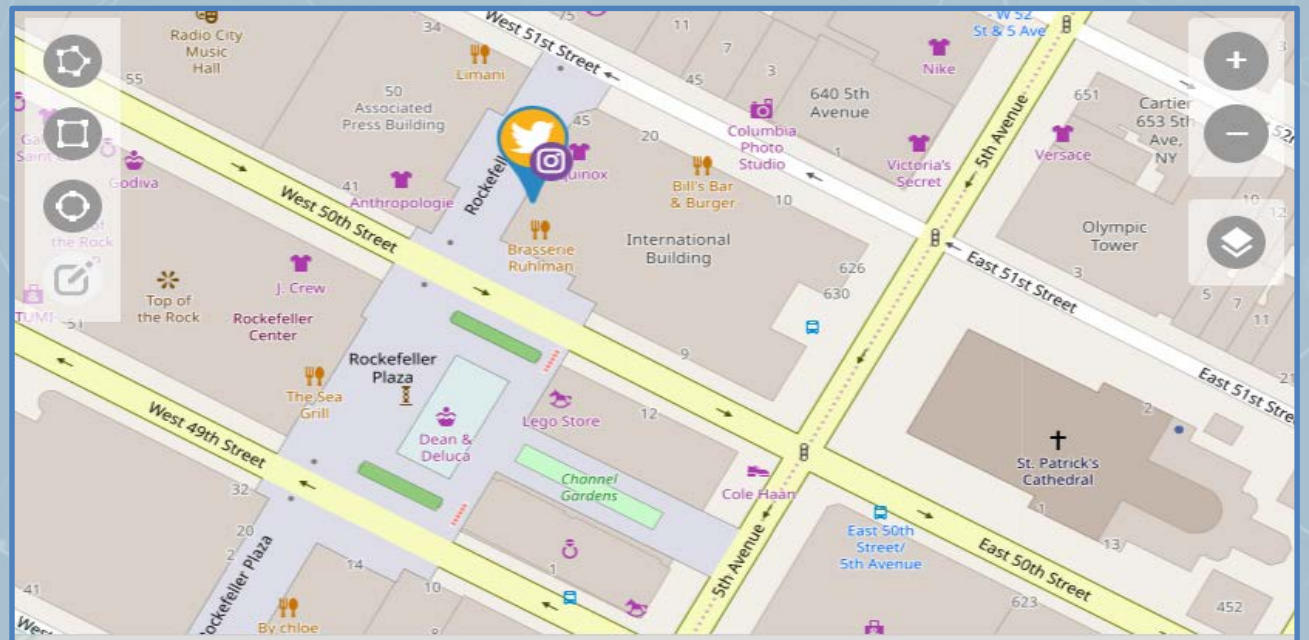
Meta Data

Source:
Instagram

Language:
en

Physical Address:
36-68 79th St Transverse, New York, NY 10024, USA

Echosec



Hetherington Group posted on Instagram 2 months ago

Hetherington Group
HetheringtonGrp
1.4k followers
Manhattan, NY
February 27th 2019, 10:07 pm

Rachel and me... red - white - blue and tan!
#roadwarriorconfessions @ Limani NYC https://t.co/mlr8IMnKrB

REPLY RETWEET 1 LIKE MESSAGE Translate

End notes

- Be aware of the potential incriminating evidence against your client which can be found through a social media investigation.
- Question potential evidence located through a social media investigation which has not been properly documented or captured. It may not be admissible.
- To be prepared, consider conducting a social media investigation on your own client

Thank You.
Connect with Hg & Me.

www.hetheringtongroup.com
rachel@hetheringtongroup.com
rachel-kronenfeld-6911426b
HetheringtonGroup
@HetheringtonGrp

HetheringtonGroup