


## **EMERGING TRENDS AND ISSUES OPEN SOURCE INTELLIGENCE (OSINT) ONLINE AND FRAUD**

Open sources go far beyond what is available in Google, Facebook, and other popular sites. This session will look beyond the obvious social networks and similar media to locate assets, discover leaks, protect reputations, track down anonymous users, and expand the arsenal of resources available, but unknown to the fraud professional. In addition, the obvious pitfalls that most fraud professionals fall into when investigating using these new mediums—what they are missing, where they are exposing themselves, and how to investigate discreetly online—are all covered.

**CYNTHIA HETHERINGTON, CFE**  
**President**  
**The Hetherington Group**  
**Wayne, NJ**

Cynthia Hetherington has more than 17 years of experience in research, investigations, and corporate intelligence. She is the founder of Hetherington Group, a consulting, publishing, and training firm focusing on intelligence, security, and investigations. A widely published author, Cynthia authored *Business Background Investigations* (2007) and the *Manual to Online Public Records* (2008). She is the publisher of *Data2know.com: Internet & Online Intelligence Newsletter*, and has co-authored articles on steganography, computer forensics, Internet investigations, and other security-focused monographs. She is also recognized for providing corporate security officials; military intelligence units; and federal, state, and local agencies with training on online intelligence practices.

“Association of Certified Fraud Examiners,” “Certified Fraud Examiner,” “CFE,” “ACFE,” and the ACFE Logo are trademarks owned by the Association of Certified Fraud Examiners, Inc. The contents of this paper may not be transmitted, re-published, modified, reproduced, distributed, copied, or sold without the prior consent of the author.

Social Media and Online Due Diligence 

## OSINT Online

Cynthia Hetherington  
Hetheringtongroup.com

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence 

## Cynthia is a...

- Librarian
- Analyst
- Security Practitioner
- Investigator
- Author of:
  - Business Background Investigators
  - The Manual to Online Public Records
  - Web of Deceit
  - Data2Know.com: Internet & Online Intelligence Newsletter



---

---

---


---

---

---

---

---

Social Media and Online Due Diligence 

## Online Investigative Scenarios

- **Security:** Watching protestors online.
- **Loss Prevention:** Locate goods in craigslist.com and intellectual property on Myspace.com
- **Competitive Intelligence:** Google.com - confidential <company name> filetype:ppt
- **Opposition Research:** Grab Form 990's on your non-profits
- **Asset Forfeiture:** Getting divorced? Funding Terror? Hunting fraudsters?
- **Due Diligence:** Conduct due diligence quickly and cheaply.
- **Criminal Actions:** Trace cellphone, PO Box & elusive email.

---

---

---


---

---

---

---

---

Social Media and Online Due Diligence 

### The law

- Legal issues are best covered with your legal counsel.
- The law varies depending on your purpose:
  - Hiring
  - Investigations
  - Vetting
    - In Germany an employer can look at LinkedIn, but not Facebook for hiring.
- There really are no definitive rules on investigating in Social Networks anywhere on the planet.

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence 

## Open Sources

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence 

### Public Records

|  |  |
|--|--|
| <ul style="list-style-type: none"><li>• Litigation history</li><li>• Media history</li><li>• Business &amp; personal affiliations</li><li>• SEC filings</li><li>• Corporate records</li><li>• Regulatory history</li><li>• Property records</li><li>• Academic records</li></ul> | <ul style="list-style-type: none"><li>• Financial records</li><li>• Vendor &amp; supplier relationships</li><li>• Board appointments</li><li>• Liens, Judgments &amp; UCCs</li><li>• Subsidiaries &amp; franchises</li><li>• Physical assets</li><li>• Intellectual property</li><li>• Political &amp; charitable causes</li></ul> |
|--|--|

Depending on the country public records do exist but are not as readily available or legal to obtain.

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence

## What can we look at in open source?

The screenshot shows the OccupyWallStreet website with a navigation bar and a main article. The article title is "While We Watch: A New Documentary on #OWS Media. Streaming Live, April 26th, 8PM". Below the title is a video player with the hashtag #whilewewatch. The website header includes "OccupyWallStreet" and the tagline "The revolution continues worldwide!".

---

---

---

---

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence

## Domaintools.com

The screenshot shows the Domaintools.com website. The main heading is "We know it all. You can too." Below this are navigation tabs: HOME, RESEARCH, MONITOR, BUY DOMAINS, LEARN, and OPEN AN ACCOUNT. A prominent section states "DomainTools has the most comprehensive collection of domain name ownership records in the world!" and lists services like Whois Lookup, Reverse Whois, and Domain Availability. A search box is visible with "occupywallst.org" entered.

---

---

---

---

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence

## Proxy'ed Domain

The screenshot shows a WhoisGuard domain lookup for "OCCUPYWALLST.ORG". The domain ID is D162782714-LROR. Registration details include: Created on 14-Jul-2011 11:47:00 UTC, Last Updated on 30-Dec-2011 01:50:15 UTC, Expiration Date on 14-Jul-2012 11:47:00 UTC, and Sponsoring Registrar as eNom, Inc. (R39-LROR). The registrant information is protected. A list of search terms is provided in a box:

- Words to look for:
- WhoisGuard
- Domains by Proxy
- Protected
- Secure
- Private

---

---

---

---

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence

### Scroll up and look for the tabs

Whois Record | Site Profile | Registration | **Server Stats** | My Whois

Reverse Whois: "WhoisGuard" was found in about 1,496,274 other domains  
NS History: 2 changes on 3 unique name servers over 1 year  
IP History: 4 changes on 3 unique IP addresses over 1 year  
Whois History: 123 records have been archived since 2011-07-19  
Reverse IP: 3 other sites hosted on this server.

Log In or Create a FREE account to start monitoring

**WHOIS FOR WINDOWS** FREE LOOKUP TOOL **DomainTools** Get it NOW

Select Server Stats Then click the IP Address

Server Type: nginx/0.7.67  
IP Address: **173.231.134.109** Reverse-IP | Ping | DNS Lookup | Traceroute  
ASN: AS29791  
IP Location: New York - New York - Voxel Dot Net Inc  
Response Code: 200  
Domain Status: Registered And Active Website

---

---

---

---

---

---

---

---

---

---

IP Information for 173.231.134.109

IP Location: United States New York Voxel Dot Net Inc  
ASN: AS29791  
IP Address: 173.231.134.109  
Reverse IP: 4 websites use this address. (examples: donnellyweb.com pibrotest.org natzotest.org occupywallst.org)

NetRange: 173.231.128.0 - 173.231.191.255  
CIDR: 173.231.128.0/18  
OriginAs: AS29791  
Netname: VOXEL-ISP-9  
NetHandle: NET-173-231-128-0-1  
Parent: NET-173-0-0-0  
NetType: Direct Allocation  
Comment: Re-assignment data at whois.voxel.net:4321.  
Comment: Abuse complaints to abuse@voxel.net.  
RegDate: 2010-03-22  
Updated: 2012-03-02  
Ref: http://whois.arin.net/rest/net/NET-173-231-128-0-1

OrgName: Voxel Dot Net, Inc.  
OrgId: VDM-1  
Address: 29 Broadway  
Address: 30th Floor  
City: New York  
StateProv: NY  
PostalCode: 10006  
Country: US  
RegDate: 2000-05-04  
Updated: 2011-09-11

Leads!

---

---

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence

### Check out Donnellyweb.com

Registrant:  
donnelly, Sean  
1 E 35th Street  
Apt 5A  
Manhattan, NY 10016  
US

Domain Name: DONNELLYWEB.COM

Administrative Contact, Technical Contact:  
donnelly, Sean seanbeachff@hotmail.com  
1 E 35th Street  
Apt 5A  
Manhattan, NY 10016  
US  
2122138004 fax: 509-471-7617

---

---

---

---

---


---

---

---

---

---

Social Media and Online Due Diligence 

### Public Information

- Business profile
- Academic history
- Business connections
- Personal affiliations
- Hobbies
- Sports teams
- Opinions
- Work schedule
- Height, weight, gender
- Travel schedule
- Caffeine or no?
- Intellectual property
- Political & charitable causes
- Photos of yourself, your family and friends
- Videos inside facilities
- Where you are and what you are doing every minute of the day!
- Updates on family events
- Drug habits
- Illnesses
- Sexual preferences

---

---

---


---

---

---

---

---

Social Media and Online Due Diligence 

### No one seems concerned

- Children are posting
  - Predators
- Business Professionals are posting
  - Competitors and Bosses are watching
- Everyone's posting
  - Reality TV meet Reality Blogger

Some examples of over exposure!

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence 

### The Weakest Link



- **Vincent\_** "Make everyday the best day of your entire life!!!!"
- Male 24 years old
- Clifton, NEW JERSEY  
Works for Large German Manufacturing Company
- Former Marine

Are those network schematics?

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence 

### Hello?



- **Employed by:**
- Large German Manufacturing Company
- Passaic, NJ, US
- Computer Programmer
- 01/04.....CURRENT

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence 

### Meet Peter from Happy Family Company



- Male 22 years old
- Los Angeles, CA
- **HFC Feature Animation**
- Burbank, CA, US
- Programmer, Editorial/Post-Production Technical Department
- **Lawrence Livermore National Laboratory**
- Livermore, CA, US
- Computer Programmer Intern, Defense Nuclear Technology
- **Peter's packing!**

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence 

## Social Network Searches

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence

### Going beyond Google

- myspace.com
- orkut.com
- technorati.com
- lcerocket.com
- Ebay.com
- Flickr.com
- friendwise.com
- Blogs.com
- lococitato.com
- yoname.com
- youtube.com
- twitter.com
- kiwipulse.co.nz
- Hi5.com
- Feedfinder.com
- Archive.org
- Zoominfo.com
- Xanga.com
- Guidestar.org
- Facebook.com
- Linkedin.com
- Spoke.com
- Spokeo.com
- Match.com
- Cuil.com
- Alt.com
- Bebo.com
- Imeem.com
- Delver.com

---

---

---

---

---

---

---

---

---

---

LinkedIn profile for Sean Dennehy. Current position: Web 2.0 Evangelist at US Government, Washington D.C. Metro Area. Education: University of Notre Dame. Recommended by 1 person. 29 connections. Industry: Defense & Space. Public Profile: http://www.linkedin.com/pub/514061ba.

---

---

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence

### Zabasearch.com – US Public Records

Zabasearch.com search results for TABEQ SALAH. Address: HOME, VA, 22019. Phone numbers: (443) 632-2881, (443) 632-2882. Includes a map and premium information for purchase.

---

---

---

---

---

---

---

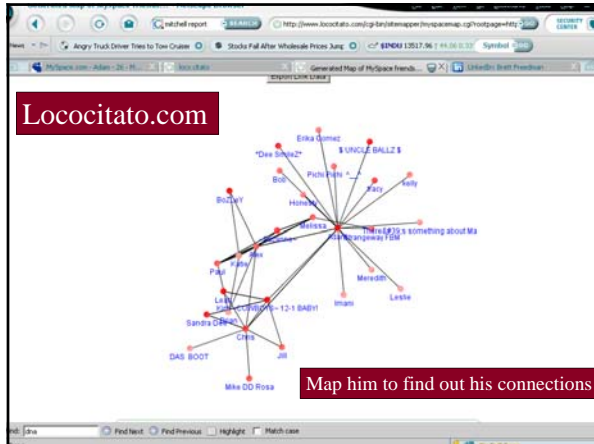
---

---

---







---

---

---

---

---

---

---

---



---

---

---

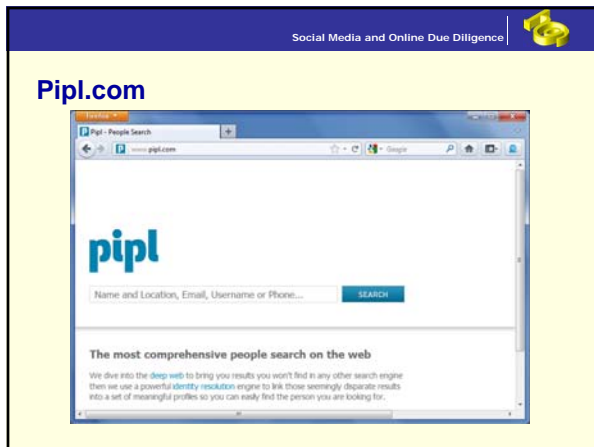
---

---

---

---

---



---

---

---

---

---

---

---

---

Social Media and Online Due Diligence 

### Social Network Searching & Tracking

- Bing.com/social – Any mention on Facebook & Twitter
- Pipl.com – Locate profiles in Social Networks
- Icerocket.com – Twitter and Myspace searches
- Spokeo.com – Search and Track
- Monitter.com – Search and Track Twitter Users
- Yoname.com – Search (email searching notifies the email address you searched)

---

---

---


---

---

---

---

---

Social Media and Online Due Diligence 

### Videos

- Youtube.com
  - You can search directly in the largest network of video material available.
- Video.google.com
  - If you don't have access to Youtube, go to its parent google. In addition to youtube, google captures videos from other feeds, so it's a bigger search!

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence 

### Photos

- Photobucket.com
- Picasa.com
- Flickr.com
- Images.google.com and images.bing.com
  - Remember to search by name, company name, username and everything else that identifies that subject.

---

---

---

---

---

---

---

---

Social Media and Online Due Diligence 

***Thank you!***

**Cynthia Hetherington**  
Hetherington Group  
ch@hetheringtongroup.com  
973-706-7525

Join us for a two day Expert Searcher Symposium  
June 14<sup>th</sup> & 15<sup>th</sup> - Fisherman's Wharf, San Francisco  
Details @ Smarteracademy.com

---

---

---

---

---

---

---

---