

SOCIAL MEDIA INVESTIGATIONS: DON'T MISS THE BOAT

PRESENTED BY: JOSEPH JONES
CERTIFIED SOCIAL MEDIA INTELLIGENCE EXPERT



SOCIAL MEDIA INVESTIGATIONS
SURVEILLANCE/ SUBROSA
RECORDS RETRIEVAL
PROCESS SERVING
ASSET LOCATES
COURT FILING

www.BoscoLegal.org
Company License # PI 14169

OBJECTIVES

- Help you see why SMI's are important
- Help you see why they need to be done properly
- Provide you with some basic tools and skills

WHY SHOULD YOU BE CONDUCTING SMI'S

➤ Facebook: 2 billion active monthly users



➤ Twitter: 1.3 billion registered users, 100 million daily users

➤ Instagram: 500 million monthly active users



➤ LinkedIn, Pinterest, Snapchat, Flickr, YouTube, Reddit, Vine, Tumblr, Google+, VK, and on and on.....

WHAT KINDS OF THINGS ARE PEOPLE POSTING?

- Where they are going
- What they are doing
- Family relationships
- Social relationships
- Work information
- Romantic relationships
- Religious views
- Political views
- Racist viewpoints
- Crimes they are committing



HOW EVIDENCE COLLECTION HAS CHANGED

- Surveillance v. SMI
 - SMI produces the same and sometimes better intel
 - SMI make surveillance more productive
- The “Person of Interest” effect
 - This is basically the same kind of work we’ve always done, just in a different way.
- Anything found with SMI is EVIDENCE!!!



HOW TO LOCATE EVIDENCE

- Avoid using unlawful methods
 - i.e. "friending" represented parties or guessing passwords
 - **DO NOT** use your personal account
 - Either use a blank account or a good "decoy"
- **REAL** internet searching
 - Using OSINT tactics
 - Boolean search terms - use your " " and *
- Thoroughly searching the accounts of friends and family members
- Searching for "no-public" content

HOW TO LOCATE EVIDENCE

For those who think their Facebook content is "Private"

<https://findmyfbid.com/>

- www.facebook.com/search/usernumber/photos-of
- www.facebook.com/search/usernumber/photos-commented
- www.facebook.com/search/usernumber/stories-by
- www.facebook.com/search/usernumber/stories-tagged

HOW TO FIND DELETED POSTS

- Deleted content won't be available on most of the major platforms.
- Look for who else might have what you're looking for.
- Can't retrieve, but active monitoring may be able to preserve them.
 - Ms. Drunk and disorderly and her uncle
- The way back machine

PROPER PRESERVATION

- **NO SCREEN PRINTS!!!**
- Document who found the evidence, when they found it, and how they found it
- Extract metadata
 - MD5 Hash = 32 character hexadecimal string AKA digital fingerprint
 - The who, when, and where of the post

RAW METADATA EXAMPLE

```
"is_video": false, "id": "451536449482933633", "display_src": "https://scontent-lax3-1.cdninstagram.com/t51.2885-15/e15/11313453_1630060443905573_1247486747_n.jpg?ig_cache_key=NDUxNTM2NDQ5NDgyOTMzNjMz.2"}]], "blocked_by_viewer": false, "followed_by_viewer": false, "is_verified": false, "has_blocked_viewer": false, "is_private": false, "external_url": null}}], "qe": {"profile": {"p": {"chaining": "false"}, "g": "control"}, "su_universe": {"p": {}, "g": ""}, "us": {"p": {"use_continue_text": "true"}, "g": "continue_vs_signup_text_test_03"}, "freq": {"p": {}, "g": ""}, "us_li": {"p": {}, "g": ""}, "discovery": {"p": {}, "g": ""}}, "display_properties_server_guess": {"viewport_width": 2133, "pixel_ratio": 0.8999999761581421}, "config": {"viewer": {"username": "shawnramirez12", "has_profile_pic": true, "profile_pic_url": "https://scontent-lax3-1.cdninstagram.com/t51.2885-19/13413444_599695090207555_1570917682_a.jpg", "full_name": "Shawn Ramirez", "id": "3439646013", "biography": null, "external_url": null}, "csrf_token": "DlAo50qoTtpl29y9DSIumcc123164Nle"}, "environment_switcher_visible_server_guess": true};</script>  
<script src="//instagramstatic-a.akamaihd.net/h1/bundles/en_US Commons.js/176aa09c1e02.js" type="text/javascript" crossorigin="anonymous"></script>  
<script src="//instagramstatic-a.akamaihd.net/h1/bundles/en_US ProfilePage.js/2edbe14fc4f0.js" type="text/javascript" crossorigin="anonymous"></script>  
  
<script>  
!function(f,b,e,v,n,t,s){if(f.fbq)return;n=f.fbq=function(){n.callMethod?n.callMethod.apply(n,arguments):n.queue.push(arguments)};if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0';n.queue=[];t=b.createElement(e);t.async=!0;t.src=v;s=b.getElementsByTagName(e)[0];s.parentNode.insertBefore(t,s)}(window,document,'script','//connect.facebook.net/en_US/fbevents.js');  
  
fbq('init', '1425767024389221');  
  
fbq('track', 'PageView');  
  
</script>  
</noscript>
```

CLEAN METADATA EXAMPLE

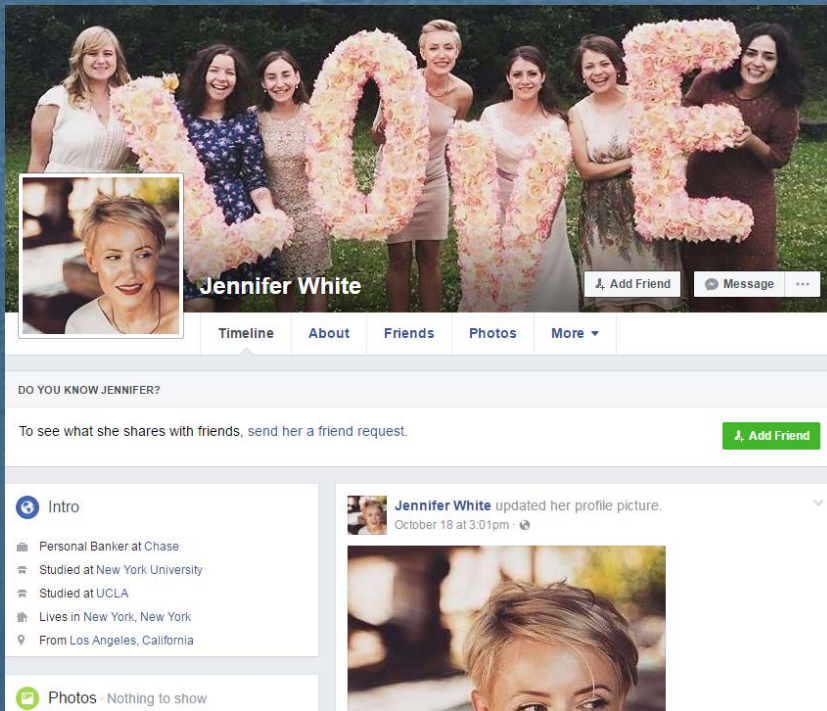
Public Account - @blssmi

[HawkingMetaData0000000001 Preview](#)

Item ID: HawkingMetaData0000000001 / Metadata

Field Name	Value
Date Created	5/8/2013 2:10:46 PM
DB Item Type	media
User ID	330206168
Relevant Account	3625798409
Account Type	1
Content Ingestion Time	11/1/2016 12:26:25 PM
Instagram UID	451537167128348047_330206168
Media Type	image
Instagram Tags	
Author ID	330206168
Author	Stephen Hawking
Author Account	stephenhawkingwag
# Comments	311
MD5 hash	8C3C53BB7D6D944628D4B0C2637C5BB2
Location Name	
Account Name	blssmi
Location Description	
Location Geo	
Caption	
Link	https://www.instagram.com/p/ZELqIBkkWP/

SPOT THE FAKE



Jennifer White Add Friend Message

Timeline About Friends Photos More

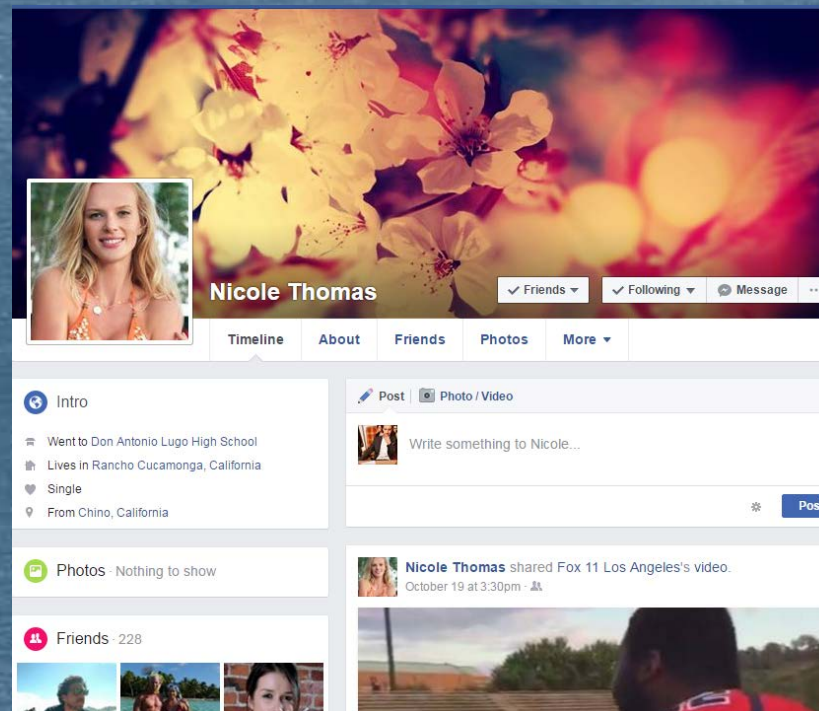

DO YOU KNOW JENNIFER?
To see what she shares with friends, send her a friend request. Add Friend

Intro

- Personal Banker at Chase
- Studied at New York University
- Studied at UCLA
- Lives in New York, New York
- From Los Angeles, California

Photos - Nothing to show

Jennifer White updated her profile picture. October 18 at 3:01pm



Nicole Thomas Friends Following Message

Timeline About Friends Photos More

Intro

- Went to Don Antonio Lugo High School
- Lives in Rancho Cucamonga, California
- Single
- From Chino, California

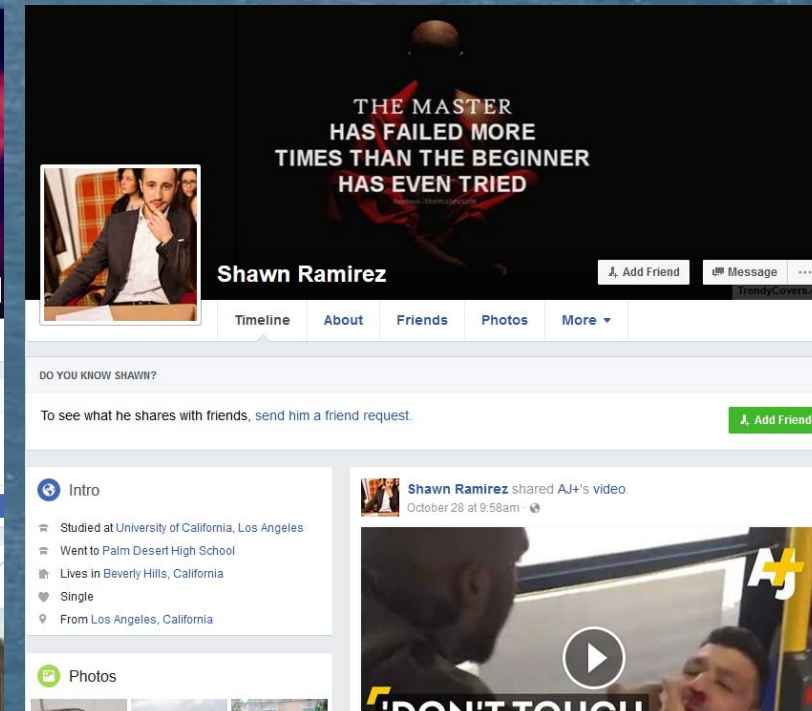

Photos - Nothing to show

Friends - 228

Post Photo / Video

Write something to Nicole... Post

Nicole Thomas shared Fox 11 Los Angeles's video. October 19 at 3:30pm



Shawn Ramirez Add Friend Message

Timeline About Friends Photos More


DO YOU KNOW SHAWN?
To see what he shares with friends, send him a friend request. Add Friend

Intro

- Studied at University of California, Los Angeles
- Went to Palm Desert High School
- Lives in Beverly Hills, California
- Single
- From Los Angeles, California

Photos

Shawn Ramirez shared AJ+ video. October 28 at 9:58am



PROPER AUTHENTICATION

- How do you know an account wasn't hacked or that it's not a fake profile?
- Post/User ID
- Review account for "specific indicia"
- Photos, friends, family, specific details of their life
- Obtain IP address/ registrant information

HAZARDS OF DOING AN "AMATEUR" SMI

- By the time the information becomes relevant, it might be gone
- Ineligibility to testify
- Good content missed
- Information mis-interpreted
- Authentication issues



CASE LAW RE: INTERNET/SOCIAL MEDIA INVESTIGATION

- **Moroccanoil V. Marc Anthony Cosmetics-** Screenshots of Facebook posts are inadmissible
- **Tienda v. State Of Texas-** Specific indicia used to authenticate social media evidence
- **Thompson v. Autoliv asp, Inc.-** Requests for production must be narrowly construed
- **Romano v. Steelcase Inc.-** Parties must turn over posts if requested properly
- **Katz v. United States-**use of decoy accounts is acceptable

www.boscolegal.org/case-law-relevant-social-media-investigations

SUBPOENAS FOR SOCIAL MEDIA INFORMATION

- Stored Communications ACT – SCA (18 U.S. Code 2701)
 - Protects personal information stored by ISP's
 - Prohibits ISP's from knowingly disclosing information—18 U.S. Code 2702(a)
 - Only exception is disclosure to government for criminal investigations
- Can Only Be Issued For Subscriber Information:
 - Name, Address, IP Address, Length of Service, and Telephone Number
- Ways Around It:
 - Federal Rule of Civil Procedure 34: communication subject to discovery
 - Flagg v. City of Detroit: court can compel originator to direct ISP to release information as normal discovery procedure
 - Court may compel ISP provider to produce information

ATTORNEY'S - CLIENTS AND LEGAL ADVICE

- Lester v. Allied Concrete Co., a Virginia state court reduced a jury award by over \$4 million dollars and ordered the plaintiff and his counsel to pay the defendants over \$700,000 in fees and expenses because of deliberate deletion of Facebook photos responsive to discovery requests
- Rule of Professional Conduct 4-3.4
 - A lawyer can't be involved in concealing evidence
- Clients should be advised to preserve Social Media Evidence (preservation letter is your CYA)

CONTACT INFORMATION

Joseph Jones, Vice President

Bosco Legal Services, Inc.

(877) 353-8181

joe@boscolegal.org

www.linkedin.com/in/pijosephjones

www.BoscoLegal.org

ADDITIONAL RESOURCES

- **Google** Subpoena Information Link:
<https://support.google.com/faqs/answer/6151275?hl=en>
- **Facebook** Subpoena Information Link:
<https://www.facebook.com/help/473784375984502>
- **Instagram** Subpoena Information Link:
Same as Facebook now that it owns Instagram
- **Twitter** Subpoena Information Link:
<https://support.twitter.com/articles/41949>

ADDITIONAL RESOURCES

- Overview of why SMI is important

<https://www.boscolegal.org/legal-services/social-media-investigations>

- In depth article including additional case law

<https://www.boscolegal.org/social-media-investigations-the-facts/>

- Comparison of Surveillance and SMI

<https://www.boscolegal.org/files/2016/04/The-New-Surveillance-v5.jpg>