OBJECTIVES

➢ **Help you see why Social Media Investigations (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: 2.2 billion active monthly users**

➢ **Twitter: 1.3 billion registered users, 335 million monthly users**

➢ **Instagram: 1Billion 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 vs. SMI**

  o **SMI produces the same types of intel as surveillance and frequently it produces even better intel**
  o **SMI makes surveillance more productive**

➢ **The "Person of Interest" effect**

  o **This is basically the same kind of work we've always done, just in a different way**

➢ **Anything found with SMI is <u>EVIDENCE</u>!!!**

How To Locate Evidence

➢ **Before you start**
  - ○ No hacking….
  - ○ **DO NOT** use your personal account
  - ○ Either use a blank account or a good "investigation" account (See Katz vs United States)

➢ **REAL** internet searching
  - ○ Boolean search terms - use your " " and NEAR(15)
  - ○ Using OSINT tactics

➢ Thoroughly searching the accounts of friends and family members

For those who think their Facebook content is "Private"

➢ **Searching for "non-public" content**

  ○ **Richards vs. Hertz - There is no expectation of privacy for SM content**

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**

➤ **You can't retrieve deleted posts, but through active monitoring you may be able to preserve them**

  ○ **Ms. Drunk and disorderly and her uncle**

➤ **The Way Back Machine**

P R O P E R P R E S E R V A T I O N

➢ **NO SCREEN PRINTS!!!**

➢ **Moroccanoil vs. Marc Anthony Cosmetics - Screenshots of Facebook posts are inadmissible**

➢ **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**

Example of Raw Metadata

```
"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>
```

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	stephenhawkingswag
# Comments	311
MD5 hash	8C3C53BB7D6D944628D4B0C2637C5BB2
Location Name	
Account Name	blssmi
Location Description	
Location Geo	
Caption	
Link	https://www.instagram.com/p/ZELqlBkkWP/

P ROPER A UTHENTICATION

➢ **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"**
  ○ **Tienda vs. State of Texas - Specific indicia used to authenticate social media evidence**

➢ **Photos, friends, family, specific details of their life**

➢ **Obtain IP address/ registrant information**

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 vs. 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 vs. 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) 353-8281

joe@boscolegal.org

www.linkedin.com/in/pijosephjones

www.BoscoLegal.org

ADDITIONAL RESOURCES

○ **Case Summaries for all things SMI**

www.boscolegal.org/case-law-relevant-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

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