Social Media Investigations: Gun Recovery Unit Edition

Detective Sergeant [Redacted] JTTF
Attention Gun Recovery Unit!!!

I am teaching this class as a supplemental to your current knowledge base of social media. It was designed using best practices acquired over my time doing social media investigations. Things we are going to cover today:

- Personal Use of the Social Media
- Legal Process Pitfalls (and how to avoid them)
- Online Covert Accounts
Understanding the Anti-Customer (everything is going to be OK, guys)
Personal Use of Social Media

We are getting crushed by Internal Affairs and Citizen Complaints on how we conduct ourselves in our personal lives. Understand that every conversation you make could be screen captured and taken out of context.
Personal Use of Social Media

There is no such thing as a secret group on social media. Be cognizant that anything you say even in jest can be taken out of context and exploited.
Personal Use of Social Media

Path of least resistance: Do not use social media while on duty.
Personal Use of Social Media

Understand as a member of the Metropolitan Police Department, any comments you make reflect on the Department. Context and humor are subjective.
Personal Use of Social Media

This includes blogs and media outlets.

BLOOMINGDALE, CRIME, TRUXTON CIRCLE

“After the suspect refused to follow numerous commands, two officers discharged their firearms”

Prince Of Petworth February 5, 2021 at 9:30am
Personal Use of Social Media

Practice operational security in your personal life
Personal Use of Social Media

Do not post any work-related content that involves crime scenes, tactics, or investigations.
Personal Use of Social Media

Don’t use personal accounts or private workspace for investigations
Media Contacts through Social Media

Defer to the PIO

DON'T DO IT

PLEASE DON'T DO IT
Legal Process for Social Media
Legal Process and Getting What you Want

• There are three types of legal process that an Investigator will find themselves issuing in an investigation. Those are:

  • 1) Preservation Letters
  • 2) Search Warrants
  • 3) Emergency Disclosures
Legal Process and Getting What you Want

Preservation Requests

↑ 18 U.S.C. §2703(f)(1) states: “A provider of wire or electronic communication service or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.”

- Good for at least 90 days
- Retroactive
- Customer not notified
Legal Process and Getting What you Want

Preservation Requests

<table>
<thead>
<tr>
<th>Case</th>
<th>Reference</th>
<th>Status</th>
<th>Account</th>
<th>Request</th>
<th>Date Requested</th>
</tr>
</thead>
</table>

The table above represents a request for preservation of evidence. The columns include fields for case, reference, status, account, request, and date requested, but the actual content is not visible in the image.
Legal Process and Getting What you Want

Preservation Requests
Legal Process and Getting What you Want

Preservation Requests

Snipping Tool
Legal Process and Getting What you Want

Preservation Requests

Screen Recorders through phone/PC and MP4 downloads through source
Legal Process and Getting What you Want

Search Warrants
Legal Process and Getting What you Want

At this point in your career, I am not going to walk you through the warrant process. What I can do is highlight recurring issues with social media search warrants. I have made all of these mistakes myself.
Legal Process and Getting What you Want

1) Training and Experience

If you are using the phrase “training and experience,” you need to be able to articulate what training and experience you have beyond the Maurice J Turner Institute of Police Science.

**Places to get Training**

- Private Sector offerings
- Community College
- Government-affiliated offerings (NCTC, HIDTA)

If you want the training, hunt for it. If the Department won’t grant you Admin Leave, take personal leave. INVEST IN YOURSELF.
Legal Process and Getting What you Want

1) Training and Experience

If you are using the phrase “training and experience,” you need to be able to articulate what training and experience you have beyond the Maurice J Turner Institute of Police Science.

Articulating Experience

We all have life experience. In addition to on-the-job experience, your personal life plays a role in justifying that your training and experience
Legal Process and Getting What you Want

2) “I know statements”

How do you know? Is it just template language or do you actually know?

One of the reasons I create social media accounts for familiarization is to understand how communication works. I know people communicate through direct messages because I have my own account. I know the data that is collected because I read the User Agreement when I created the account.
3) Language is important

If slang is used to describe a firearm, be prepared to discuss how you know a ____ is a firearm or _____ is a shooting. Visuals and criminal records help.
Legal Process and Getting What you Want

4) High Crime Area

The Gun Recovery Unit is not the low crime response unit. If you are in area, there is probably a reason. Instead of exclusively using high crime area, articulate how you happened upon an investigation or a subject. Things that help:

- CRS Analytical Products
- Heat Maps
- Deployment Orders and historical knowledge
Legal Process and Getting What you Want

5) The social media platform rejected my warrant
Legal Process and Getting What you Want

5) The social media platform rejected my warrant

Most Common reason: wrong address/company allocation

https://www.search.org/resources/isp-list/
https://www.arin.net/
Law Enforcement Portals
Google
Legal Process and Getting What you Want

5) The social media platform rejected my warrant

Second Most Common Reason: No one caught an error on the law enforcement side.
• Does the warrant match the affidavit?
• Is the URL correct?
• Is the charge correct?
• Did you use a template?
Legal Process and Getting What you Want

Emergency Disclosures

18 U.S. Code § 2702 - Voluntary disclosure of customer communications or records

A social media platform can provide you subscriber level information on an account if you can articulate (in good faith), that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.
Legal Process and Getting What you Want

Emergency Disclosures

These should not be used in lieu of legal process. It’s a handshake agreement with a company to mitigate a threat, with the expectation that legal process will be forthcoming (if applicable).
Legal Process and Getting What you Want

Emergency Disclosures

The two requirements needed for most companies are:

- A demonstration that there is a threat
- A demonstration that the threat is imminent (not eminent)
Legal Process and Getting What you Want

Emergency Disclosures

An Emergency Disclosure may require an additional disclosure request
Legal Process and Getting What you Want

Emergency Disclosures

Document everything as part of the investigation
Be sure to follow up with legal process (Congress expects it)
Legal Process and Getting What you Want

A threat is mitigated with an arrest. If the imminent threat from 37th Place is revealed to be the 37th Place from Vero Beach, contact the Vero Beach Police Department or State Police.
Online Threats that actually Happened

Jeff Weise and Newgrounds (2005)
Online Threats that actually Happened

When: March 21, 2005
Number Killed: 9
Number Injured: 5
Killer: Jeffrey Weise
Online Threats that actually Happened

Adam Lanza and Steam (2012)
Online Threats that actually Happened

Adam Lanza Threatened Sandy Hook Killings Years Earlier, Records Show
Online Threats that actually Happened

Nikolas Cruz and Youtube (2018)
Online Threats that actually Happened

Nikolas Cruz and Youtube (2018)
Online Threats that actually Happened

Hindsight 2020
Threat Example

MPD Receives a complaint from a tipster

• When you speak to the complainant, she advises that she knows [REDACTED] from Reddit and he uses the name [REDACTED]. She advises he purports to be a [REDACTED] and provides screen captures of the threats
Threat Example

Assess and Decipher the Threat

- After reviewing the provided information, the Redditor does openly discuss plans to shoot up the
Threat Example

• Based on the [redacted] information, you determine this threat requires immediate action. You contact [redacted] to have no record of a [redacted] being banned, and you submit a preservation request to Reddit.
Threat Example

- You submit an Emergency Disclosure request to Reddit. It is granted, providing you subscriber level information on the account
Threat Example
Threat Example
Threat Example
Threat Example

- You submit an Emergency Disclosure request to Google for subscriber information on the account, who identify the user as "[redacted]" has no record of interaction
Threat Example

- You submit search warrants to Google and Reddit for the contents of the Users account.
Threat Example

- The returns provide enough information to identify the user as
Threat Example
Threat Example

Threat Mitigated

- You notify law enforcement, ___ and the tipster of the resolution.
THE FLOWCHART OF JUSTICE
Unique Threat Cases I’ve Worked
Unique Threat Cases I’ve Worked
Unique Threat Cases I’ve Worked
Social Media Scenarios: Scenario Edition

Detective Sergeant [Redacted]
Threat #1: 4Chan hates Kent, DC

- On [redacted], 4Chan user [redacted] makes threats to the District of Columbia. Mitigate!
Threat #1: 4Chan hates Kent, DC

- There is a specific date given to shoot the Kent neighborhood. You submit an Emergency Disclosure to 4Chan...and it is denied. You also submit a preservation request.
Threat #1: 4Chan hates Kent, DC

- You notify 2D of the Threat to Kent, and SOD of the threat to the FSK Bridge.
Threat #1: 4Chan hates Kent, DC

- You obtain a warrant for the account and 4Chan provides you with an IP address and more posts*
Threat #1: 4Chan hates Kent, DC

- A second warrant is submitted, and subsequently declined
Threat #1: 4Chan hates Kent, DC

- You document the incident, the declination, and you refer the available info to [redacted] (also documented)
Threat #2 A Verizon Caller hates 6D

On [redacted] a telephonic threat is made to the Sixth District, threatening to shoot everyone inside. The call comes from Verizon Wireless telephone number [redacted]

Mitigate!
Threat #2 A Verizon Caller hates 6D

Emergency Legal Process provides subscriber information on the number, revealing it to belong to a resident at
Threat #2 A Verizon Caller hates 6D

An interview with the building manager confirms the subject resides at [redacted] and an Emergency Search Warrant is obtained for the residence.
 Threat #2 A Verizon Caller hates 6D

The Search Warrant is executed, recovering multiple firearms and 3D Printing equipment. The subject is PC arrested on scene
Threat #2 A Verizon Caller hates 6D

A follow up subpoena is submitted to the telephone provider.
Threat #3: Twitter hates block parties

O [redacted] announced on Twitter that she will be holding a Mask-Free Block party in the 1800 Block of Columbia Road, with no concern for Law Enforcement. On [redacted] reports to law enforcement that she received the below hate crime threat in response. Mitigate!
Threat #3: Twitter hates block parties

You consult knowyourmeme and urban dictionary, revealing “They finna drag you” to be a “Finna Woke” reaction meme, used to suggest that someone is going to get dragged through the comments section. A cursory review of the comments from the block party announcement reveal that she was indeed dragged through the comments.
Threat #3: Twitter hates block parties

• If the user is known, interview to ensure it was just internet tomfoolery. Suggest the post be deleted.
• If there is evidence of constant harassment from the account, consider reporting it.
• Advise [redacted] of your findings, encourage her to report it.
• Report [redacted] to the 3rd District to ensure it doesn’t happen
• Document and save everything
Threat #4: [Redacted] does not like Mondays

On [Redacted] twitter account [Redacted] makes threats to shoot up a school. A cursory review of the account shows it is likely in [Redacted] but you ended up with it as a District Detective. Mitigate!
Threat #4: does not like Mondays:

The complaint was submitted anonymously.

The threat should be considered credible and imminent.
Threat #4: [Redacted] does not like Mondays

The complaint was submitted anonymously.
The threat should be considered credible and imminent.
Submit a Preservation Request and Emergency Disclosure to Twitter

Law Enforcement Request
Please fill out all the fields below so we can review your report.

Tell us about yourself

- I am an authorized law enforcement representative (e.g., police officer, federal agent).
- I am an authorized government representative (e.g., district attorney, minister).
- None of the above.

Not what you need help with? Choose another topic.
Threat #4: does not like Mondays

Submit a Preservation Request and Emergency Disclosure to Twitter

Tell us about yourself

- I am an authorized law enforcement representative (e.g., police officer, federal agent).
- I am an authorized government representative (e.g., district attorney, minister).
- None of the above.

Type of request or report

How can we help?

- Request for account information
- Non-emergency information request
- Emergency disclosure request
- Report potentially illegal content
- Report other violations
- Other inquiries
Threat #4: does not like Mondays

Submit a Preservation Request and Emergency Disclosure to Twitter

Nature of the emergency

Select all that apply
- [ ] Suicide / Self-harm
- [x] Threat to another person
- [ ] Threat to a place
- [ ] Other threat

Subject of the emergency

Full name

Identify the person(s) in danger of death or serious physical injury

Twitter username

Twitter username of the subject account(s) whose information is necessary to prevent the emergency (e.g., @safety)
Threat #4: [Redacted] does not like Mondays

Twitter provides Subscriber Information, [Redacted]
Threat #4: [Redacted]
does not like Mondays

You contact [Redacted] (speaking with a live person), and provide them with the reporting information. [Redacted] later advise that the subject was identified, interviewed, and arrested (document).
Threat #5: Craigslist Missed Connections is still a thing

On [redacted] you received a threat from the Washington DC Missed Connections section of Craigslist. Mitigate!
Threat #5: Craigslist Missed Connections is still a thing

The statement is concerning, but lacks a timeframe to show exigency.
Threat #5: Craigslist Missed Connections is still a thing

A warrant is submitted to Craigslist
Threat #5: Craigslist Missed Connections is still a thing

The warrant provides an IP address, an email address,
Threat #5: Craigslist Missed Connections is still a thing

Follow up warrants are conducted on the email address and ISP, identifying the poster as
Threat #5: Craigslist Missed Connections is still a thing

You attempt to interview him and he declines. A warrant is present and signed.
Threat #6: [Redacted] hates Gallaudet

On [Redacted], you receive a Facebook threat against Gallaudet University. Gallaudet Staff advise [Redacted] Mitigate!

E1405
Threat #6: [REDACTED] hates Gallaudet

The threat account is publically viewable, and you are able to view the threat.

Snip it! Save it! Document it!
Threat #6: [Redacted] hates Gallaudet

You submit an Emergency Disclosure request to Facebook, which is granted. A follow up ED is submitted
Threat #6: [Redacted] hates Gallaudet

Police interview the subject, who admits he did it. A warrant is submitted and signed, and Gallaudet University is advised.
Threat #7: The Flash hates PlaylistLive

On [reddacted], [reddacted] reports to DC that she has received threats from [reddacted].

Mitigate!
Threat #7: The Flash hates PlaylistLive:Answer 3C

You interview [REDACTED] revealing that the subject has contacted her via [REDACTED] separate accounts.
Threat #7: The Flash hates PlaylistLive:Answer 3B

You interviewed the subject, revealing that the subject has contacted her via 19 separate accounts.
Threat #7: The Flash hates PlaylistLive:Answer 3B

You interviewed [redacted] revealing that the subject has contacted her via 19 separate accounts.
Threat #7: The Flash hates PlaylistLive:Answer 3B

You submit an Emergency Disclosure to Facebook for all accounts.
Threat #7: The Flash hates PlaylistLive: Answer 3B
Threat #7: The Flash hates PlaylistLive: Answer 3B
Threat #7: The Flash hates PlaylistLive: Answer 3B
Threat #7: The Flash hates PlaylistLive: Answer 3B

...nd denies the incident. You call... from the numbers on his Account returns, and he admits that he made the calls due to “his problems”
Threat #7: The Flash hates PlaylistLive: Answer 3B

You obtain a warrant for a
nd follow up subpoenas are submitted to Facebook and the ISP to serve as legal process.
Use of Undercover Accounts

Why create an Online Covert Account (Undercover account)?
Use of Undercover Accounts

Social Media has become a language of its own over the last two decades. As a form of communication, it is critical to successful investigations. Things to consider:

• Undercover Accounts typically violate the User Agreement from social media platforms
• Intellectual Property is a thing
• Documentation is the fine line between focused investigations and targeted harassment.
Use of Undercover Accounts

There are two variations of an OCA, and they should be kept exclusive of each other. Overt accounts are used to monitor opensource social media, and Covert accounts are used for focused contact on predicated individuals.
Use of Undercover Accounts

Overt Accounts

• An Overt Account monitors social media that is otherwise publicly viewable. The three platforms this is most often seen in are:
  • Facebook
  • Instagram
  • Twitter
Use of Undercover Accounts

Covert Accounts

- A Covert Account is used for focused investigations. We gain information on bumping (contacting) subjects through a starting point (we need to have a reason). These starting points could include:
  - IQ Reports
  - Tips from Citizens
  - Tips from Officers
  - Social Media Aggregators
  - Hashtags or Names from your experiences as a law enforcement Officer
  - Gang Books and MPD Databases
Use of Undercover Accounts
Use of Undercover Accounts
Use of Undercover Accounts
Use of Undercover Accounts
Use of Undercover Accounts
Use of Undercover Accounts
Use of Undercover Accounts
Use of Undercover Accounts

Building Your Accounts:

With overt Accounts, no contact should be made with subjects. These are simply made to view opensource platforms. Every search or viewing merits documentation.
Use of Undercover Accounts

Building Your Accounts:

With covert Accounts, the end goal is an arrest. This may be done through an operation that introduces an Undercover or a Confidential Informant, or in the case of threats by way of a search warrant for the account.
Use of Undercover Accounts
Use of Undercover Accounts
Use of Undercover Accounts
Use of Undercover Accounts
Use of Undercover Accounts
That’s it, Amigos!

MAY THE 4TH BE WITH YOU