

October 13, 2022

Sent via DC Government Public FOIA Portal

Metropolitan Police Department
General Counsel
300 Indiana Ave., NW
Room 4125
Washington, DC 20001

RE: Freedom of Information Act Request

To Whom it May Concern:

This is a request under the District of Columbia’s Freedom of Information Act (“FOIA”), D.C. Code § 2-531 et seq., on behalf of the Brennan Center for Justice at NYU School of Law (“Brennan Center”) and Data for Black Lives (“D4BL”). Brennan Center and D4BL seek **all records concerning the Metropolitan Police Department’s (“MPD”) use of undercover and/or covert accounts from September 1, 2021 through the date of the production**. This request is set forth more fully below at pages 2-3. To aid the MPD in processing the request, we first provide the following background information.

Background

According to an MPD training presentation previously released to Brennan Center and D4BL, “Covert [undercover social media] accounts are used for focused contact on predicated individuals.”¹ MPD uses covert accounts for “focused investigations” to “gain information on bumping (contacting) subjects through a starting point,” for which officers “need to have a reason.” Ex. A at 105. The Presentation states that “with covert Accounts, the end goal is an arrest. This may be done through an operation that introduces an Undercover or Confidential Informant, or in the case of threats by way of a search warrant for the account.” *Id.* at 114. An Executive Order published in 2021 regarding social media monitoring defines an undercover

¹ Detective Sergeant [Redacted], Joint Terrorism Task Force, *Social Media Investigations: Gun Recovery Unit Edition* (the “Presentation”) at 103. The Presentation, which contains MPD’s redactions, is attached as **Exhibit A**.

account as a “social media identity that has been created by a member of MPD for the purpose of concealing his or her identify [*sic*] as a law enforcement officer in order to gain information.”²

Several public records describe the policies surrounding MPD’s use of undercover and/or covert social media accounts for police business. Criminal Intelligence Branch (“CIB”) Lieutenant Michael J. Pavlik issued a memorandum to CIB members regarding Operation Summer ICE Social Media teams in April 20, 2011 (the “2011 Memo”), attached as **Exhibit C**, which permitted the use of undercover social media accounts in connection with MPD’s summer crime enforcement initiative if a member of the social media team could make a showing of reasonable suspicion and received explicit permission from a CIB lieutenant. On June 5, 2013, the same memorandum was published as a Social Media Monitoring Policy, creating general CIB social media teams and extending the reporting requirements as applicable to all of CIB (the “2013 Memo”), attached as **Exhibit D**.

The Executive Order provided department-wide procedures for using social media in police investigations. It further specified that the use of “non-official MPD social media accounts (i.e., undercover accounts) in the course of legitimate criminal investigations or intelligence collection efforts related to public safety or potential criminal activity” was limited to the following divisions: Criminal Investigations Division, Intelligence Division, Internal Affairs Division (criminal investigations only), Narcotics and Special Investigations Division (“NSID”),³ and Youth and Family Services Division. Ex. B at 1. The Executive Order requires the creation of several written documents for MPD employees using undercover social media accounts.

Request

To reiterate, the Brennan Center and D4BL request **all records concerning MPD’s use of undercover and/or covert accounts in MPD’s control or possession from September 1, 2021 through the date of the production.**⁴ Such records include, but are not limited to:

² Chief Robert J. Contee III, Metro. Police, *Exec. Order 21-025: Social Media for Investigative and Intelligence-Gathering Purposes* (Nov. 8, 2021) (the “Executive Order”) at 3. The Executive Order is attached as **Exhibit B**.

³ It is our understanding that NSID was recently renamed as the Violent Crime Suppression Division (“VCSD”). Please construe any reference to NSID as applicable to VCSD and vice versa.

⁴ To the extent that the Executive Order did not supersede the division-specific policies and procedures described in the 2011 and 2013 Memos, the following documents would also be responsive to the request: (a) written requests from CIB social media team members to a CIB lieutenant articulating reasonable suspicion to support a member’s accessing non-public social media pages, such as those that require an invitation, approval or membership, including exigent circumstance written requests that may be submitted the following business day; (b) documentation of reasonable suspicion that the CIB lieutenant is required to keep for at least 30 days; (c) written requests to extend monitoring past 30 days; and (d)

1. All written approval requests that the Executive Order requires be sent to the NSID commander prior to using or creating an undercover account in the following divisions: Criminal Investigations Division, Intelligence Division, Internal Affairs Division, Narcotics and Special Investigations Division, and Youth and Family Services Division. *See Ex. B at 1.*
2. All documentation or logs relating to obtaining and documenting consent to use proprietary images or another person's likeness in an undercover account or profile. *See Ex. B at 2.*
3. The centralized registry of all active undercover social media accounts that NSID is required to maintain for de-confliction purposes pursuant to the Executive Order. *Id.* at 3.
4. All reports of potential compromises of online aliases that the Executive Order requires be reported to the member's commanding official immediately and all documentation of any guidance by the member's commanding official. *Id.* at 3.
5. All written approvals by a member's commanding official to use an individual's personal account for covert and/or undercover purposes, as required by the Executive Order. *Id.* at 2.
6. All documented reviews of all undercover and/or covert accounts that commanding officials are required to conduct every 30 days pursuant to the Executive Order. *Id.* at 3.
7. All documentation and presentation of training that members are required to undergo prior to using an undercover account. *Id.* at 2.

Fee Waiver and Expedited Processing Requested

The above requests are a matter of public interest. The disclosure of the public records is not for commercial purposes; instead, it will contribute to the public's understanding of police operations. Accordingly, Brennan Center and D4BL request a fee waiver and expedited processing pursuant to D.C. Code § 2-532(b).

The Brennan Center for Justice is a nonpartisan, non-profit law and policy institute dedicated to upholding the American ideals of democracy and equal justice for all. The Center has a long history of compiling information and disseminating analysis and reports to the public about government functions and activities, including policing.

Data for Black Lives is a nonprofit organization dedicated to the mission of using data and technology to make concrete change in the lives of Black people. Through advocacy, movement-building, and leadership development, D4BL supports a network of grass-roots racial justice organizations to challenge discriminatory uses of data and algorithms across systems. With a national network of thousands of activists and data-scientists, D4BL seeks to build a

weekly reports that members must share for "each OSS area" and urgent reports that must be shared ASAP. *See Ex. C at 1-2; Ex. D at 1-2.*

future where data and technology are forces for good in Black communities, instead of instruments of oppression.

Accordingly, the primary purpose of the above requests is to obtain information to further the public's understanding of important policing policies and practices. Access to this information is crucial for the Brennan Center and DB4L to evaluate such policies and their effects.

Should the Metropolitan Police Department choose to charge a fee, please inform the Brennan Center of the total charges in advance of fulfilling this request via email at levinsonr@brennan.law.nyu.edu.

Prompt Response Required

Brennan Center and D4BL appreciate the MPD's attention to this request and look forward to a response within fifteen business days of receipt (by November 3, 2022). D.C. Code § 2-532. If MPD withholds any records, please list, in writing, each document that is withheld as well as the specific claimed exemption. *Id.* § 2-533. We request that, where possible, documents be produced in electronic format. If documents must be produced in hard copy or if you have any questions concerning this request, please first contact Rachel Levinson-Waldman at (202) 249-7193 or levinsonr@brennan.law.nyu.edu.

Sincerely,

Brennan Center for Justice
Data for Black Lives

Exhibit A

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.



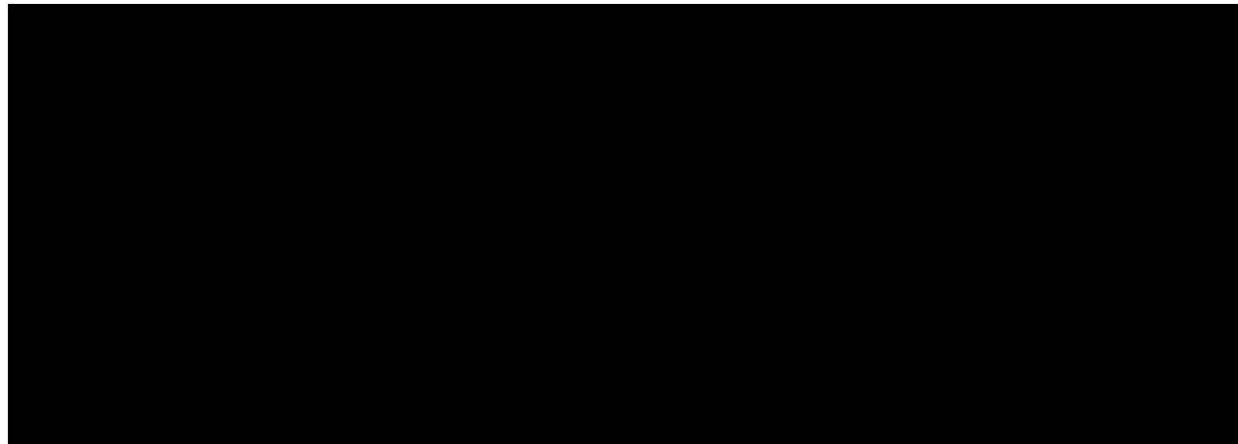
Personal Use of Social Media

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

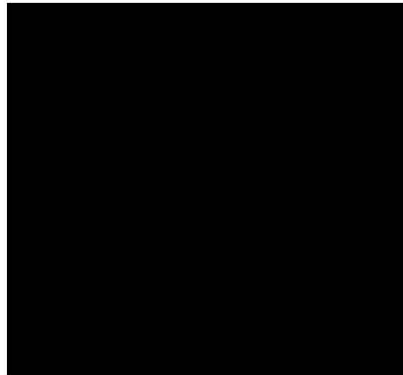
“After the suspect refused to follow numerous commands, two officers discharged their firearms”

[Prince Of Petworth](#) February 5, 2021 at 9:30am



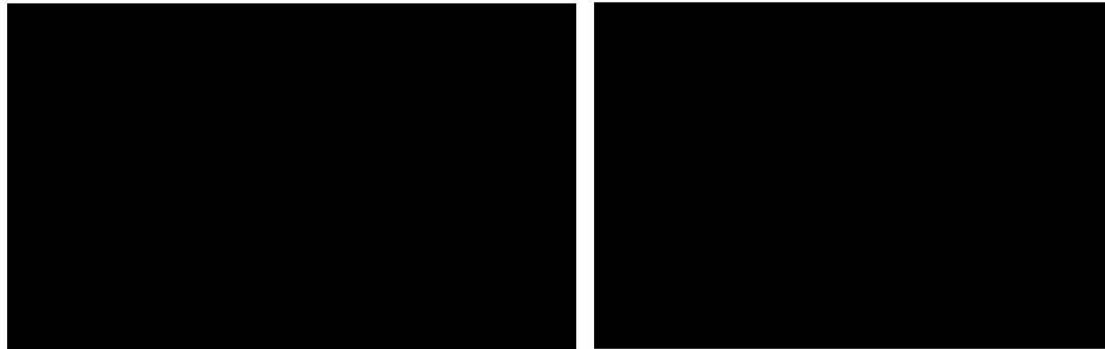
Personal Use of Social Media

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.



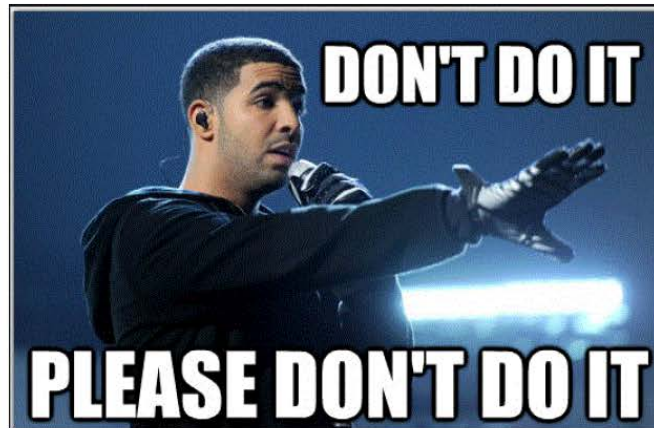
Personal Use of Social Media

Don't use personal accounts or private workspace for investigations



Media Contacts through Social Media

Defer to the PIO



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

Case	Reference	Status	Account	Request Type	Date Requested
[Redacted]					

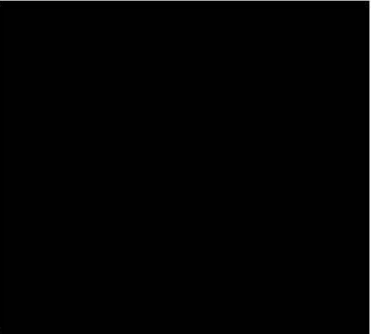


Homeland Security Bureau
Intelligence Division

300 Indiana Avenue, Suite 2000, NW, Washington D.C., 20011 (202) 724-1237 FAX (202) 727-4588

July 26, 2017

Twitter, Inc.
1355 Market Street, Suite 900
San Francisco, CA 94103



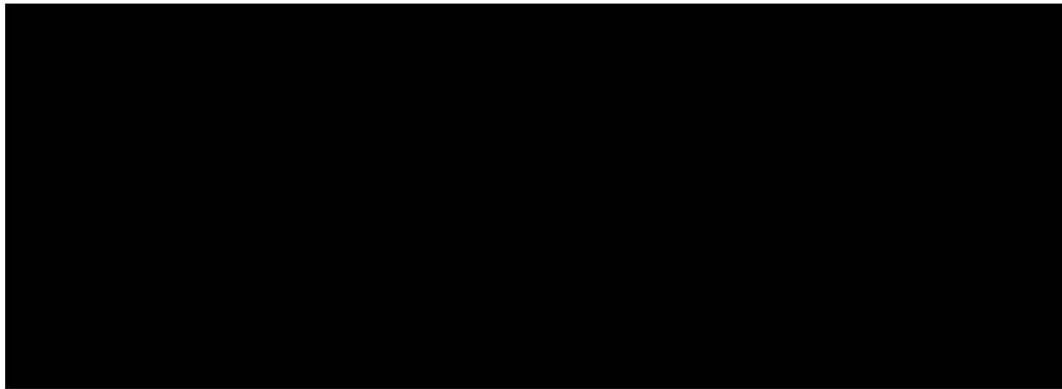
Legal Process and Getting What you Want

Preservation Requests



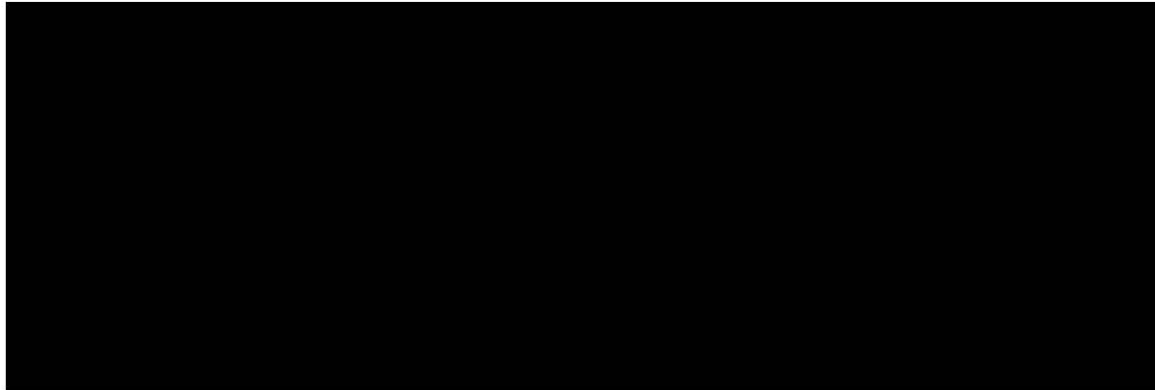
Legal Process and Getting What you Want

Preservation Requests



Legal Process and Getting What you Want

Preservation Requests



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?



Legal Process and Getting What you Want

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.

TOP DEFINITION

blickie

a [firearm](#)

After he [popped off](#) he [tosset](#) the [blickie](#) in [the river](#)

by [YoungDon609](#) December 28, 2008

91 33

FLAG

Get a **blickie** mug for your mom Yasemin.



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?

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
ONE YOUTUBE ACCOUNT PURSUANT
TO 18 U.S.C. § 2703 FOR
INVESTIGATION OF VIOLATIONS OF
18 U.S.C. §75(e)

SC No. _____

Filed Under Seal



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

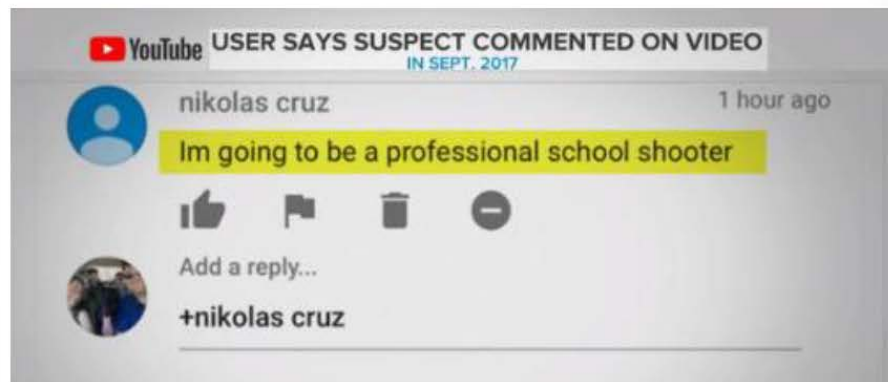


Adam Lanza Threatened Sandy Hook Killings Years Earlier, Records Show



Online Threats that actually Happened

Nikolas Cruz and Youtube (2018)



Online Threats that actually Happened

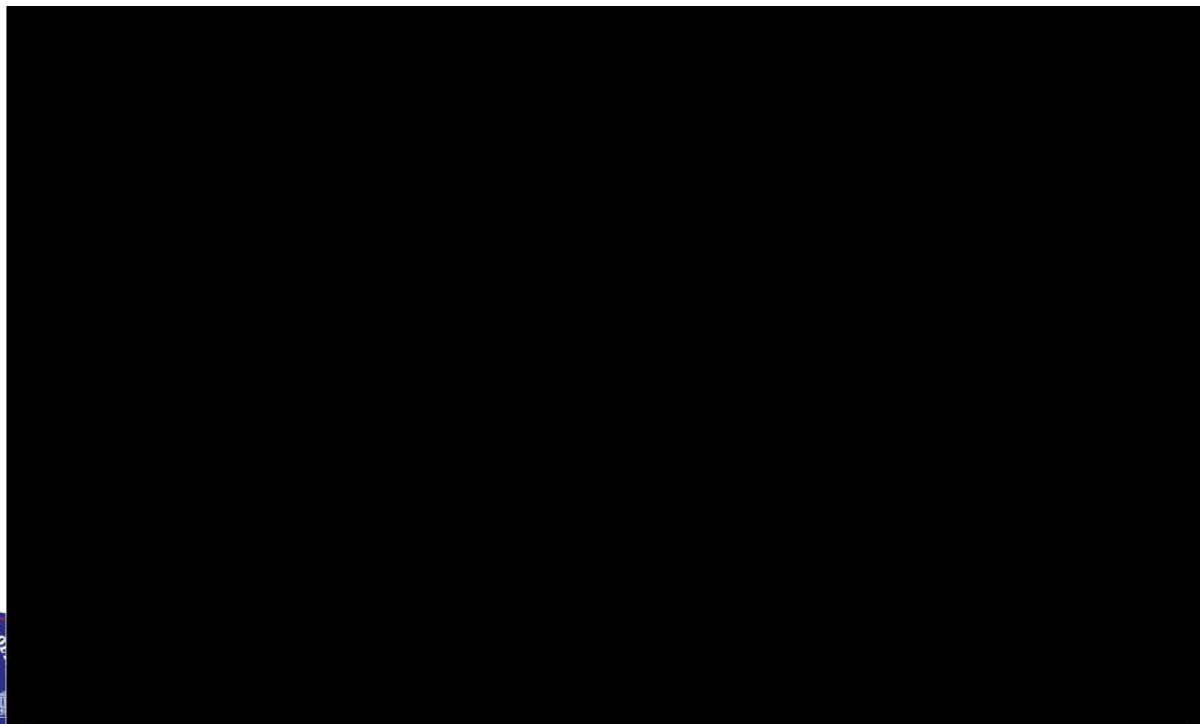
Nikolas Cruz and Youtube (2018)



Online Threats that actually Happened



Threat Example



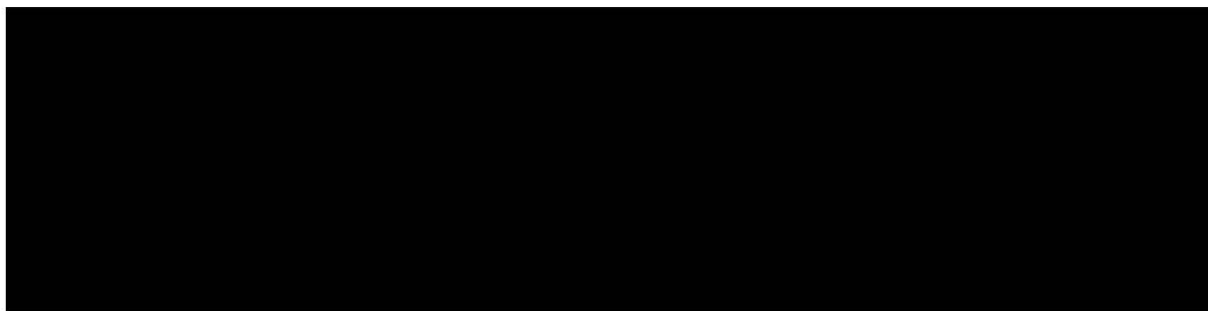
Threat Example

Assess and Decipher the Threat

- After reviewing the provided information, the Redditor THKSGIVINLEFTOVER does openly discuss plans to shoot up the Veteran Affairs Hospital.

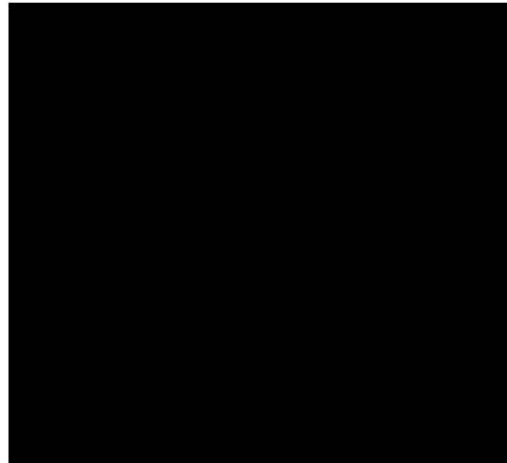


Threat Example



Threat Example

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

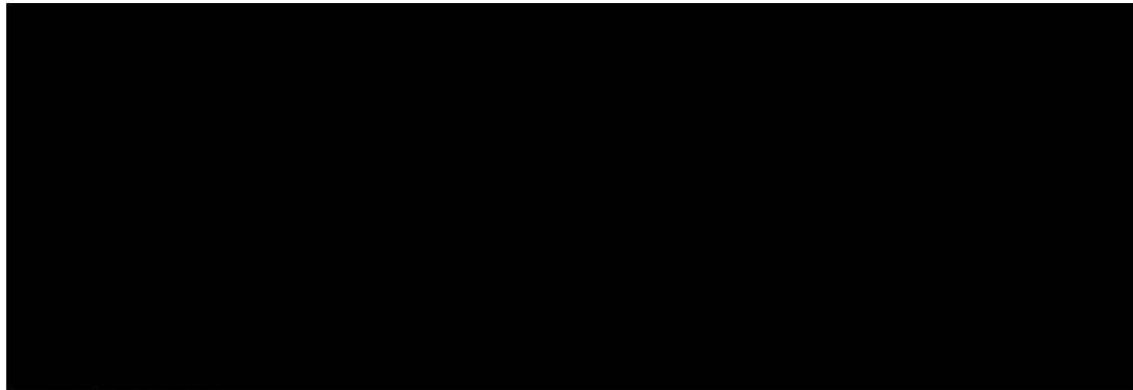


Threat Example

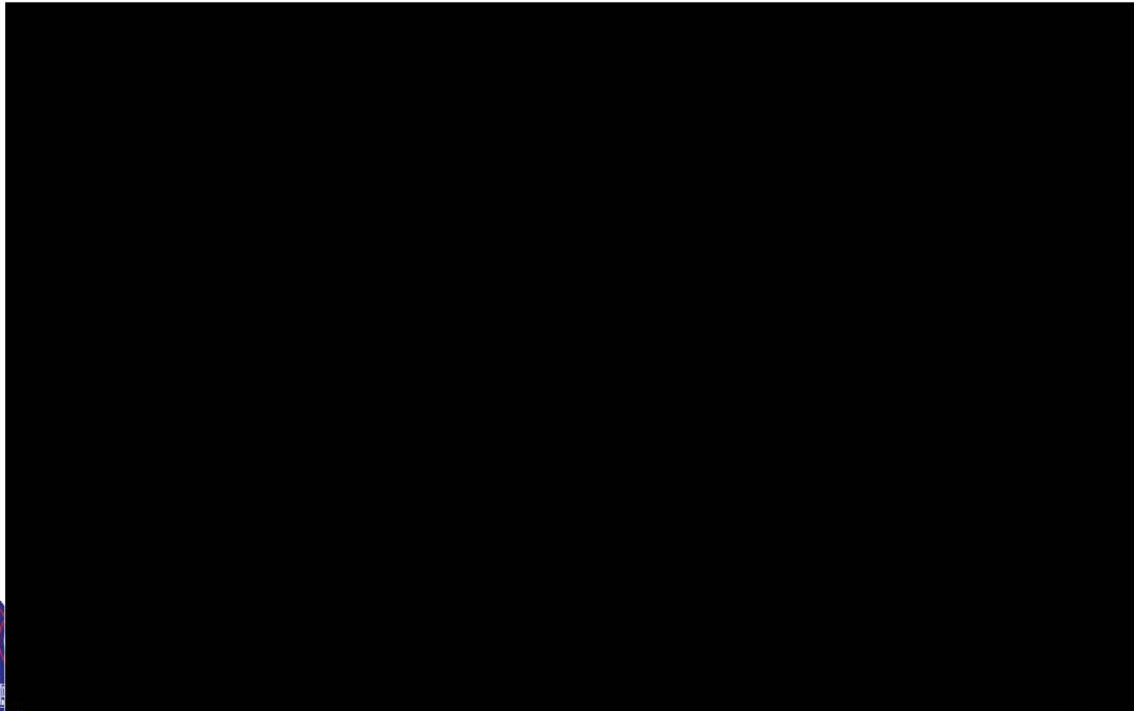


Threat Example

- You reach out to LG Dacom, whose domain master advises it is probably a US Military user

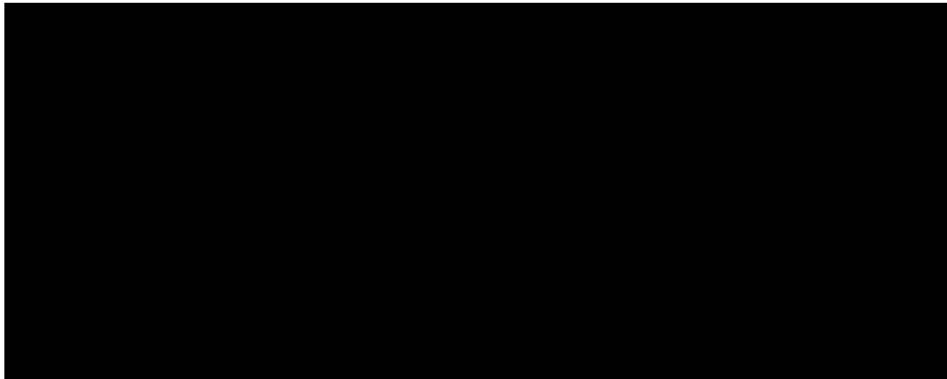


Threat Example

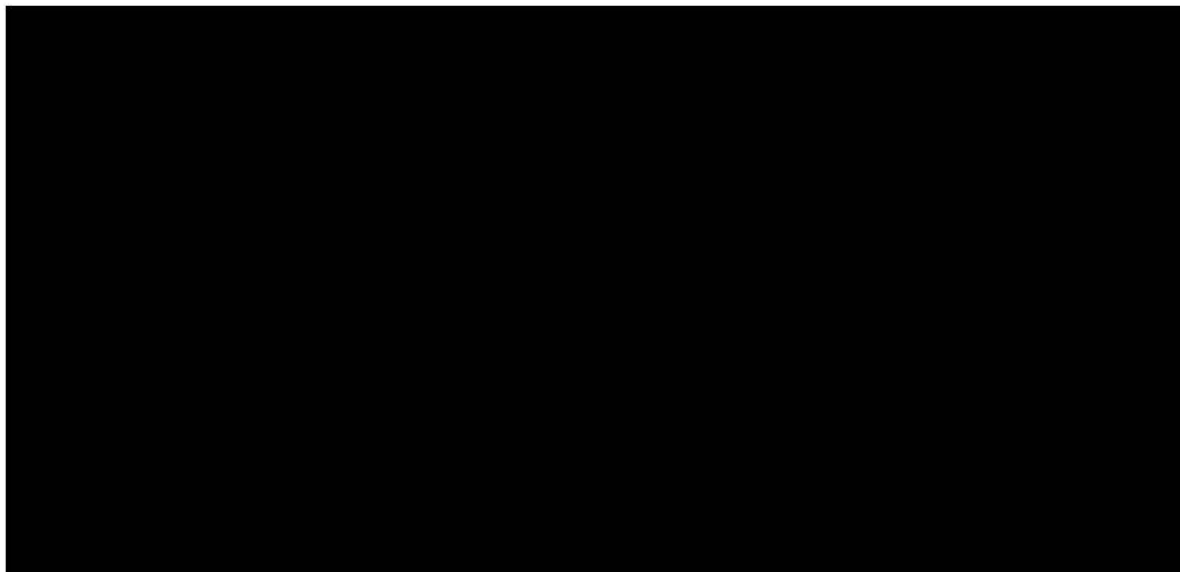


Threat Example

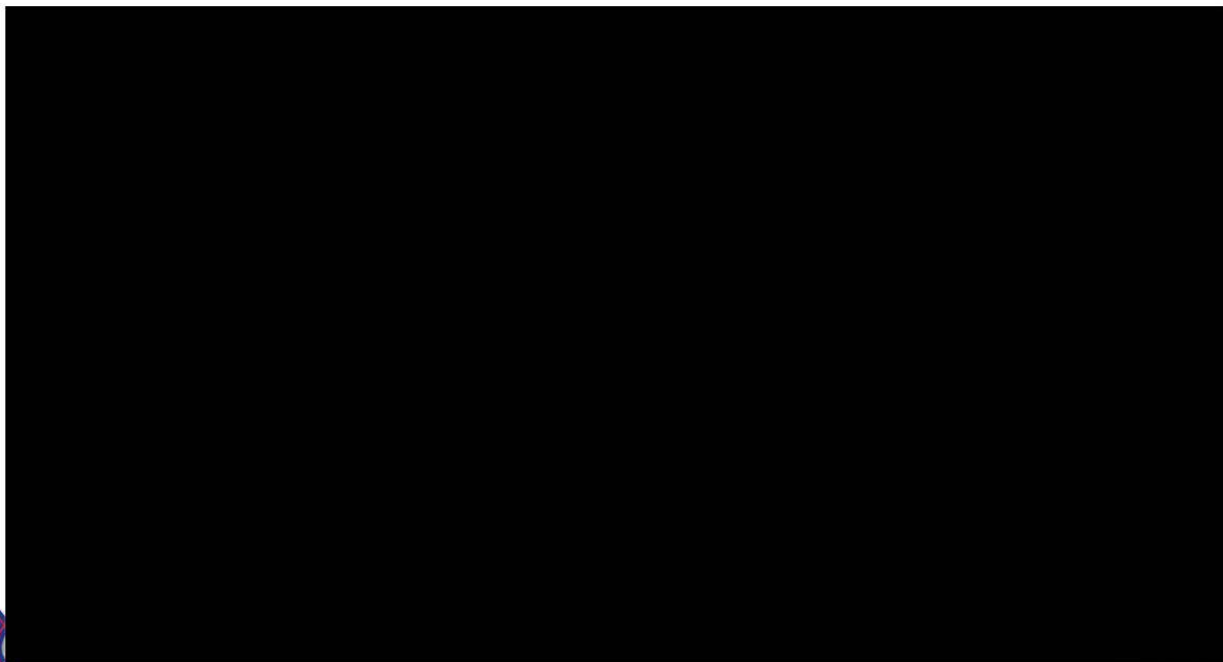
- You submit an Emergency Disclosure request to Google for subscriber information on the account, who identify the user as “Scott Ivant.” VA has no record of interaction



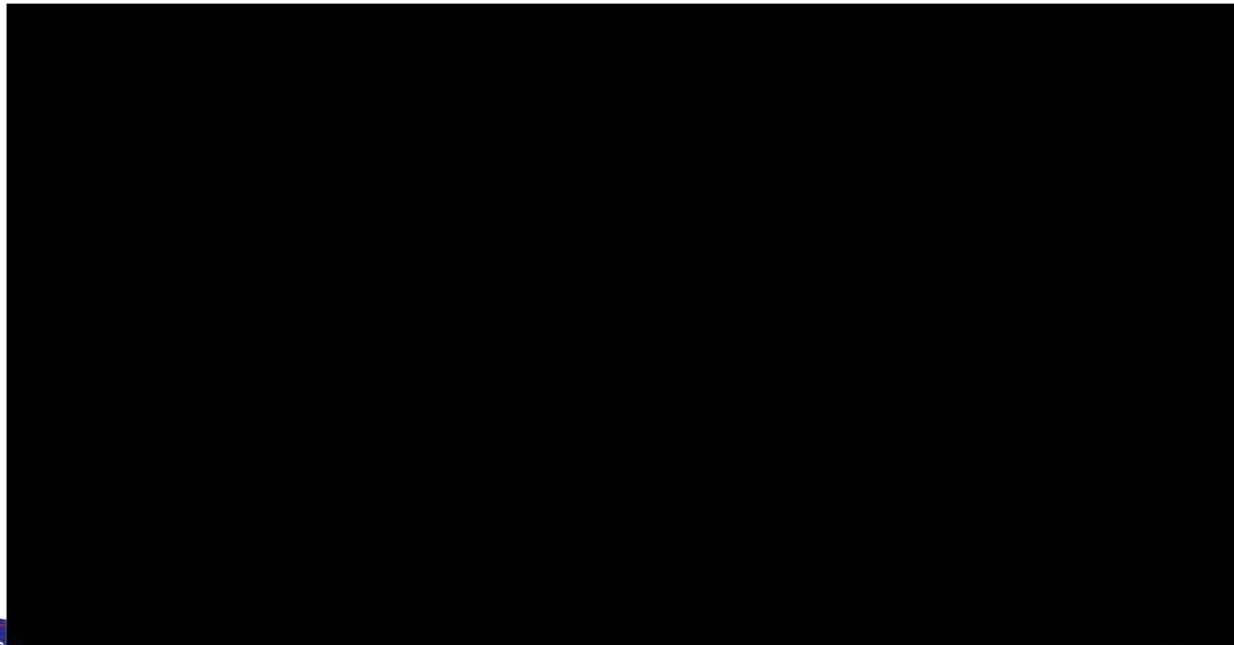
Threat Example



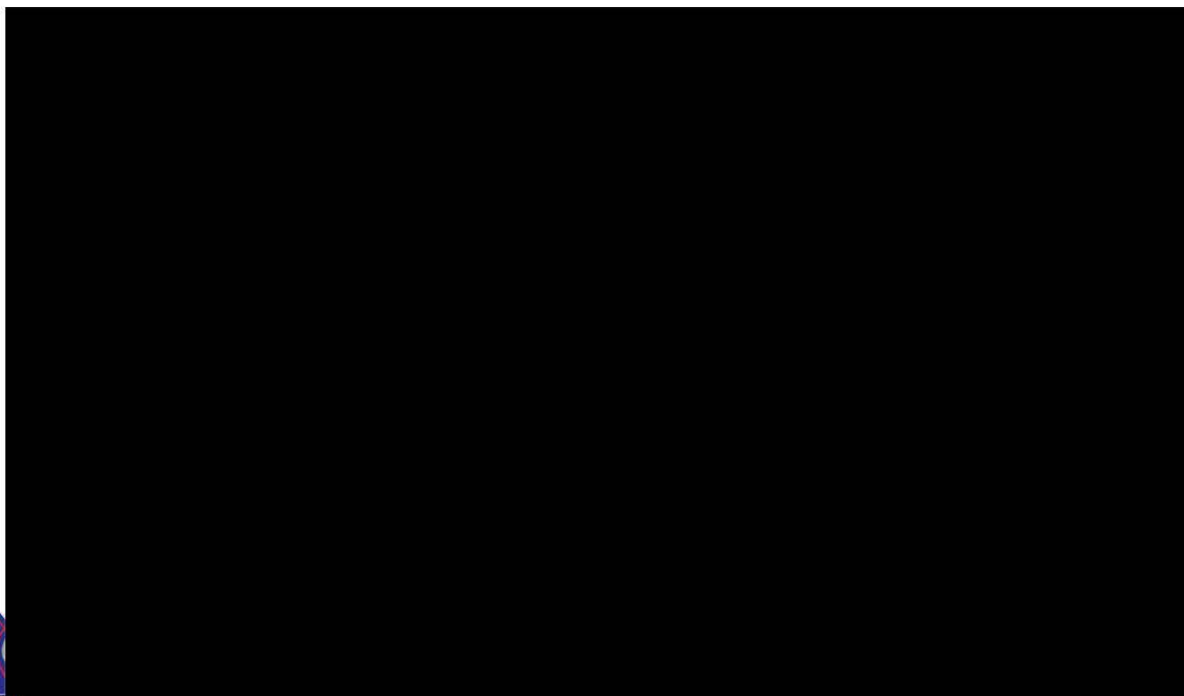
Threat Example



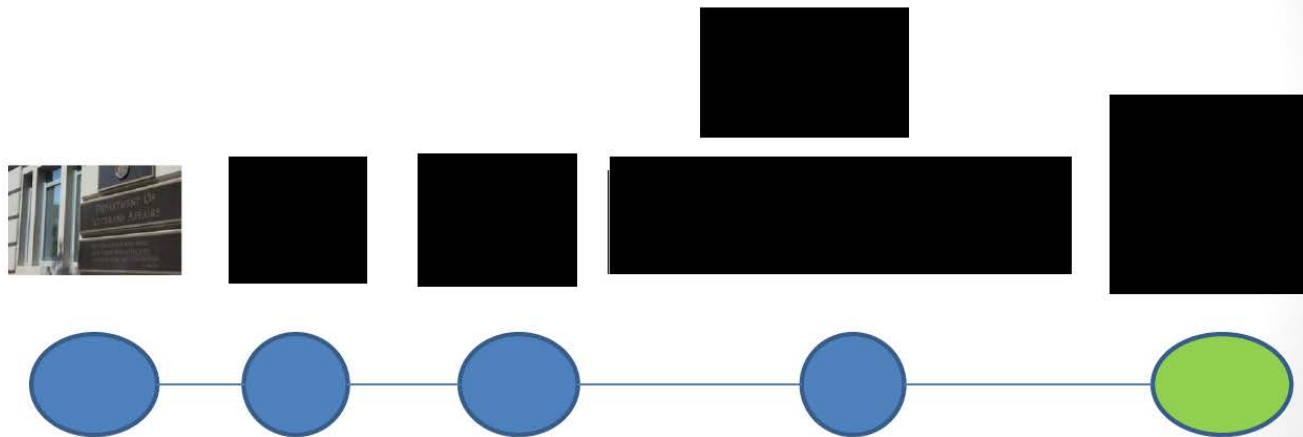
Threat Example



Threat Example



THE FLOWCHART OF JUSTICE



Unique Threat Cases I've Worked

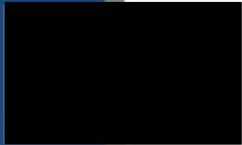
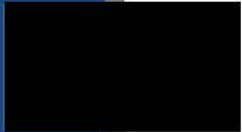
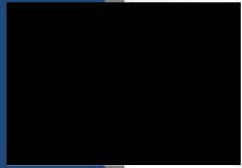


Unique Threat Cases I've Worked



Unique Threat Cases I've Worked



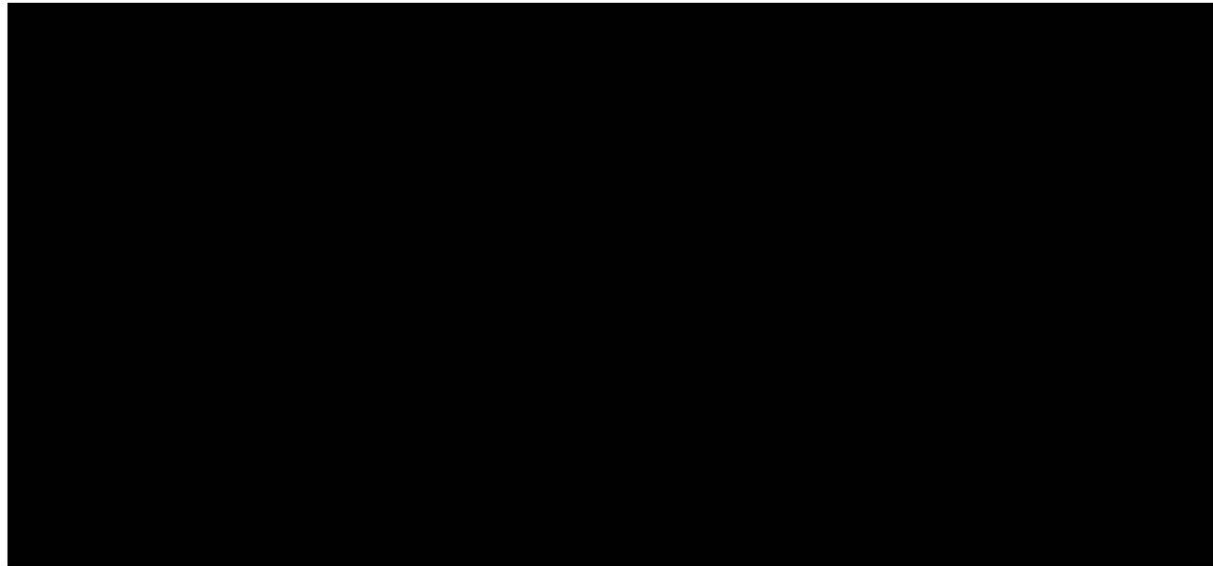


Social Media Scenarios: Scenario Edition

Detective Sergeant



Threat #1: 4Chan hates Kent, DC

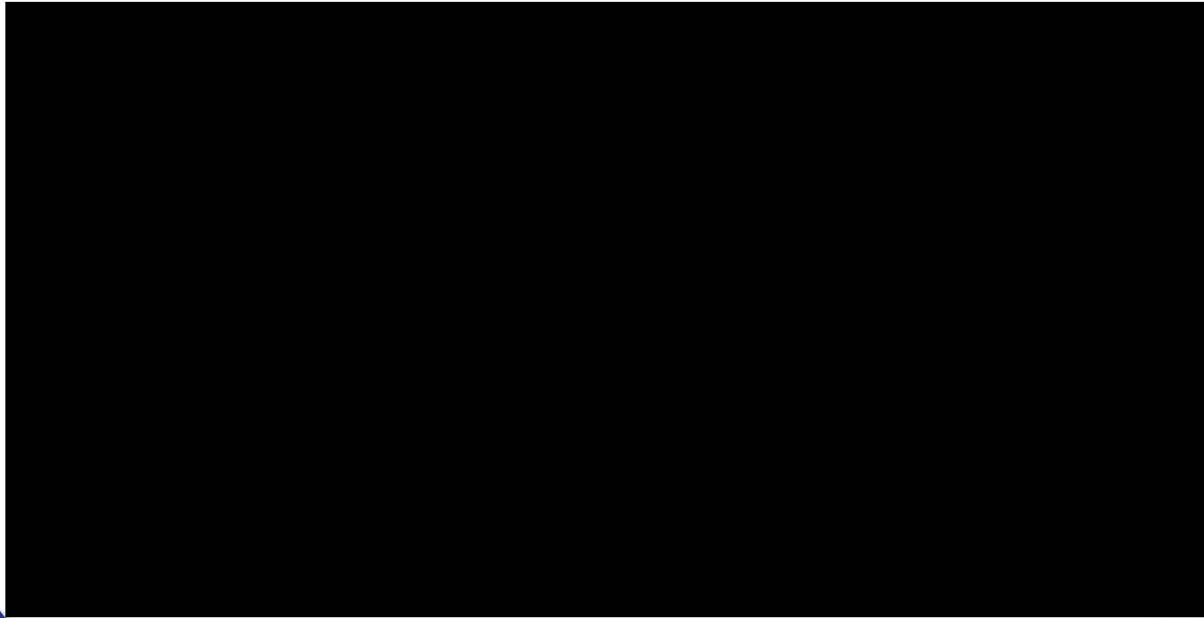


Threat #1: 4Chan hates Kent, DC

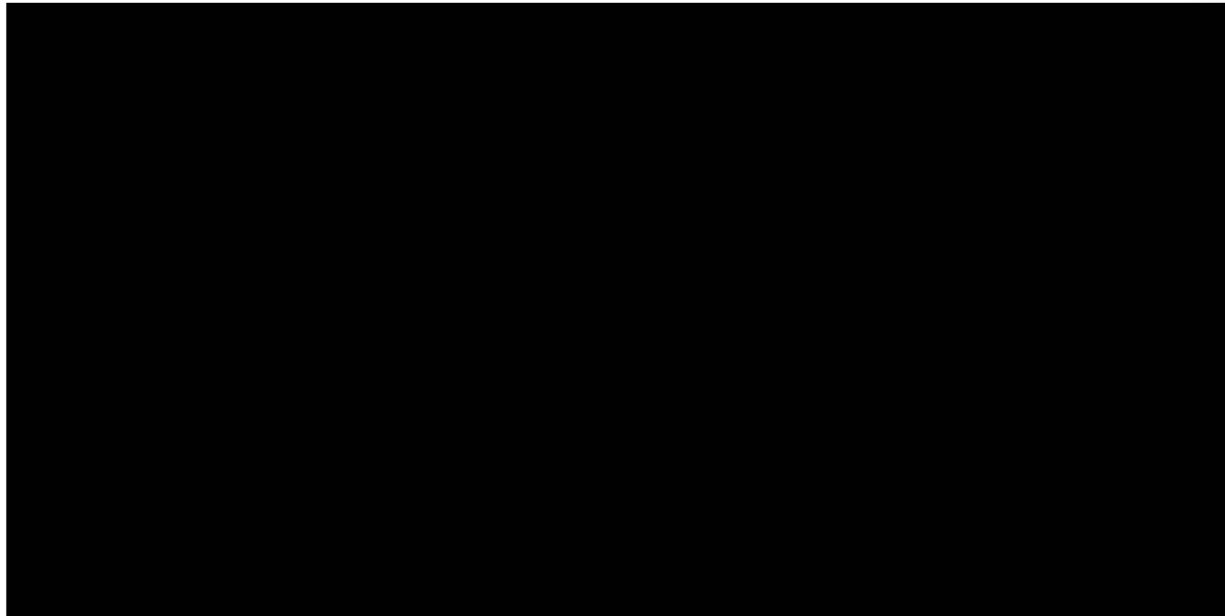
- There is a specific date given to shoot the Kent neighborhood. You submit an Emergency Disclosure to 4Chan...and it is denied. You also submit a preservation request



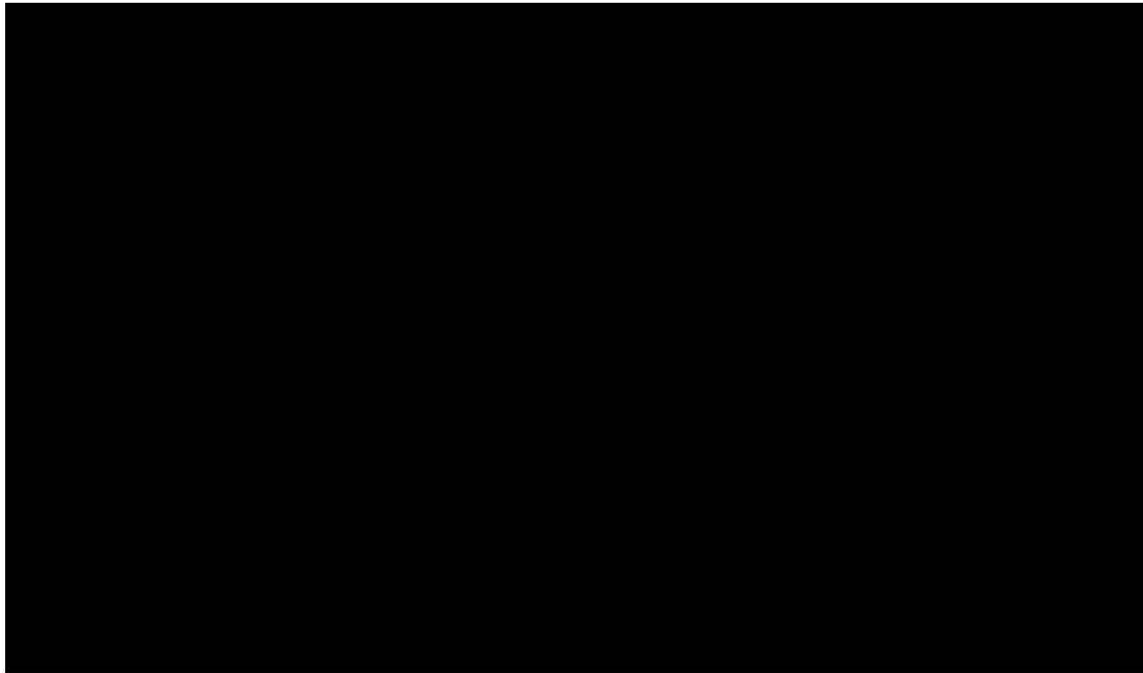
Threat #1: 4Chan hates Kent, DC



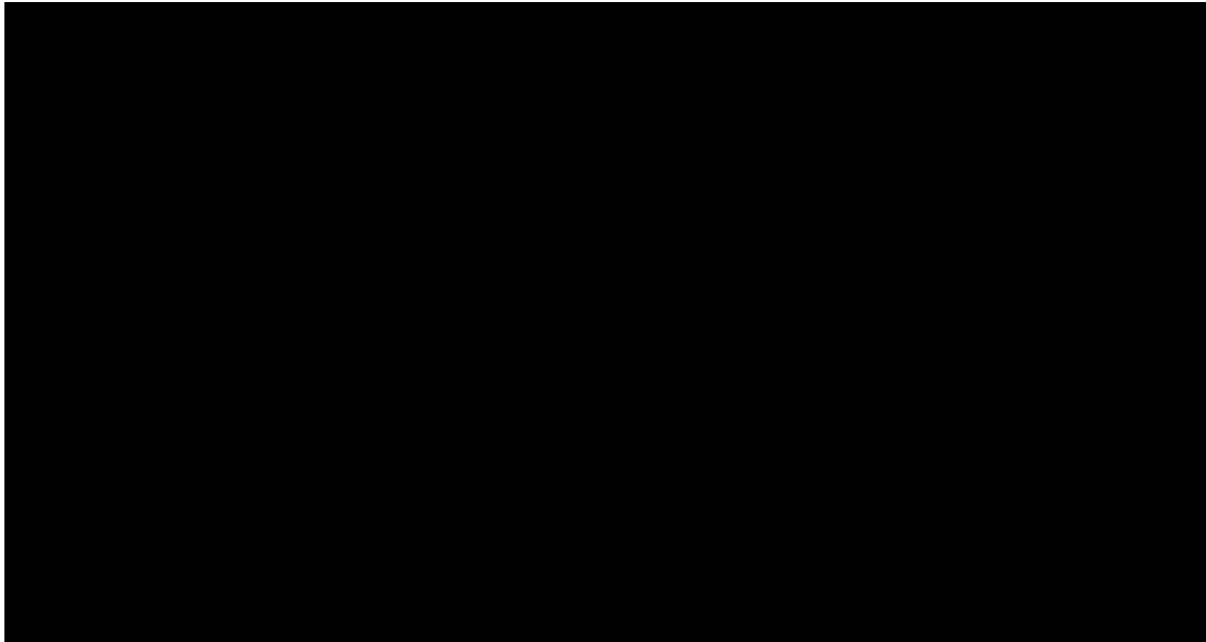
Threat #1: 4Chan hates Kent, DC



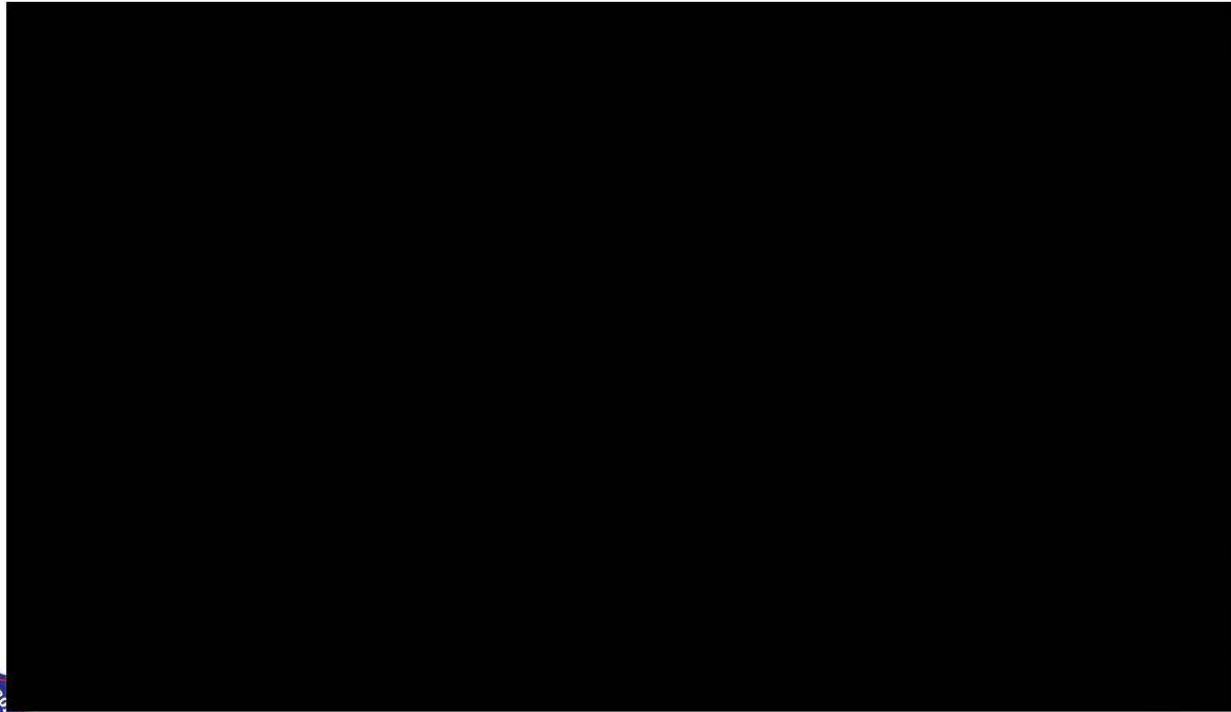
Threat #1: 4Chan hates Kent, DC



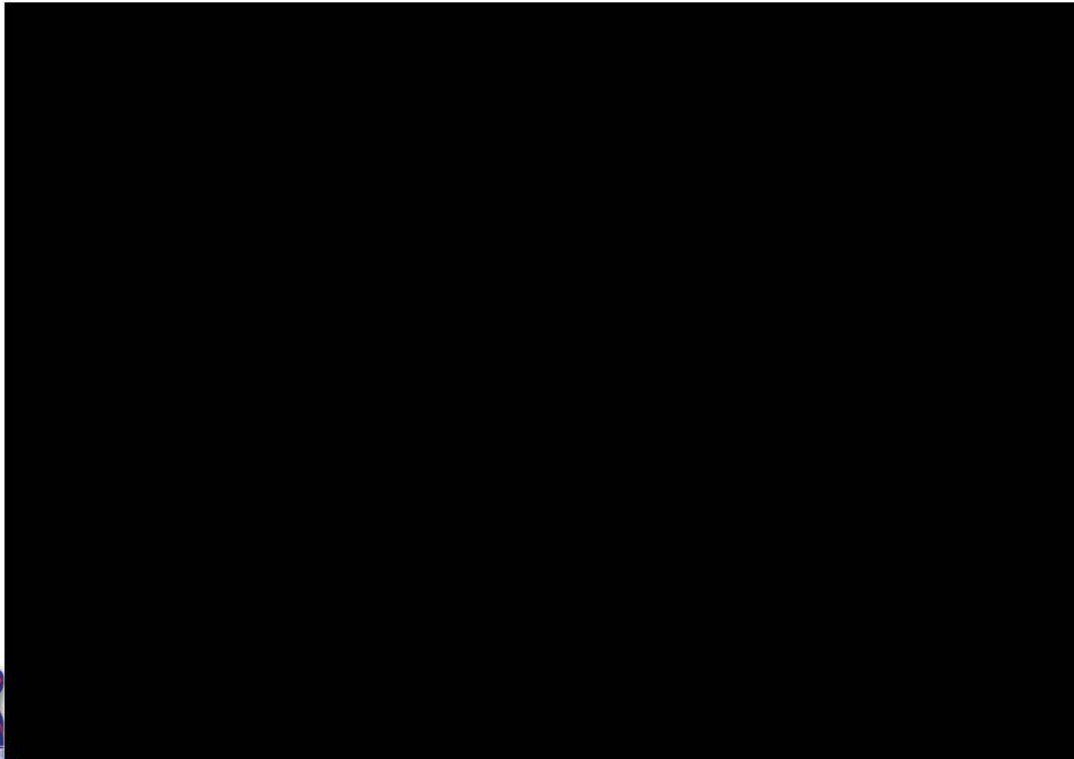
Threat #1: 4Chan hates Kent, DC



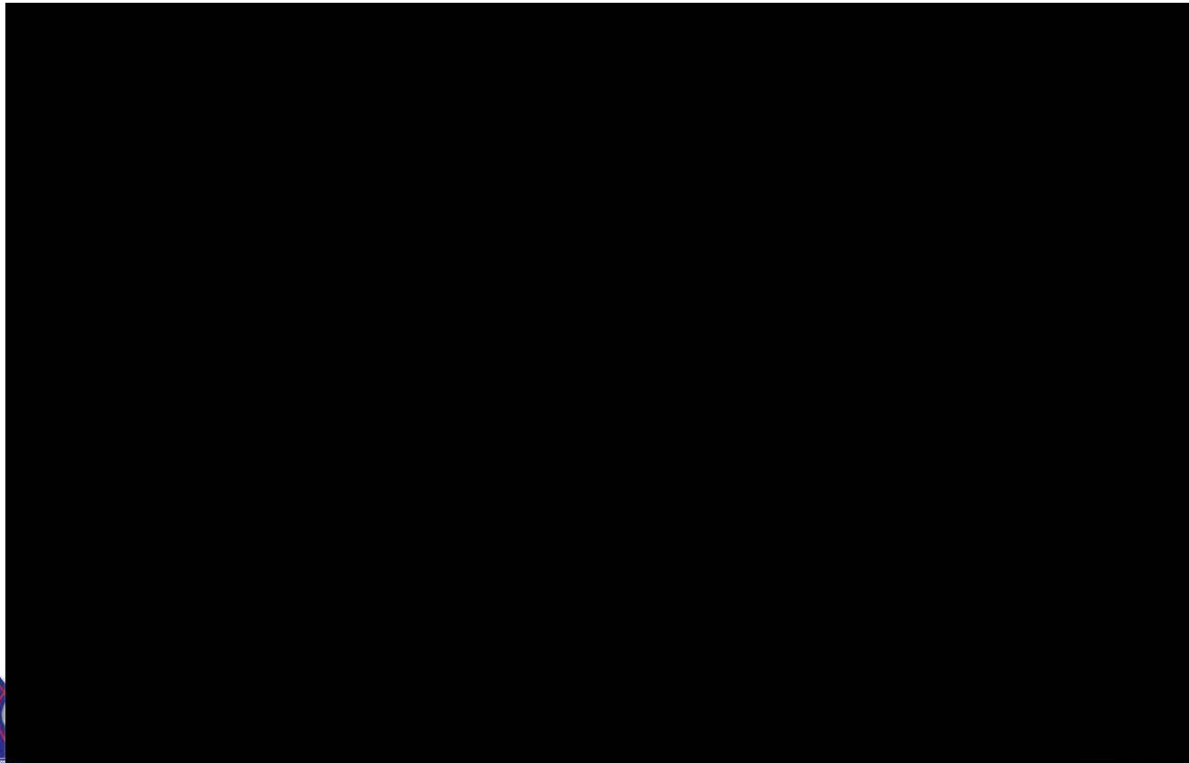
Threat #2 A Verizon Caller hates 6D



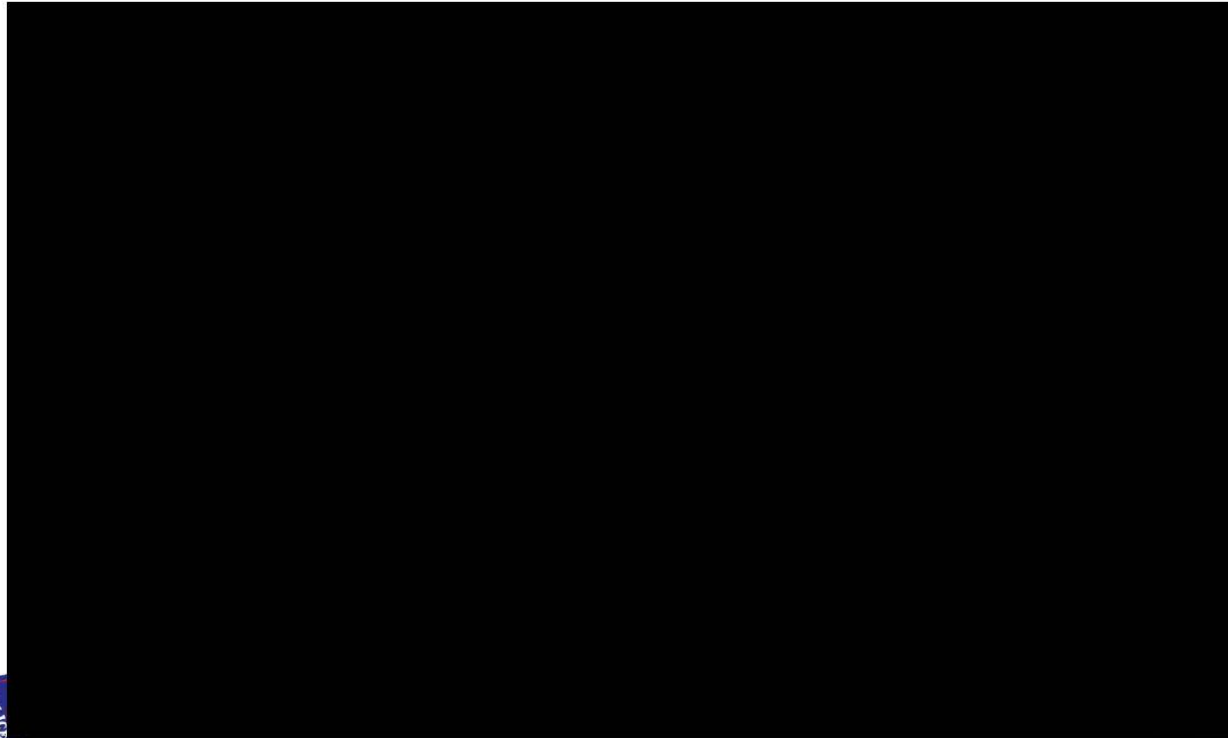
Threat #2 A Verizon Caller hates 6D



Threat #2 A Verizon Caller hates 6D



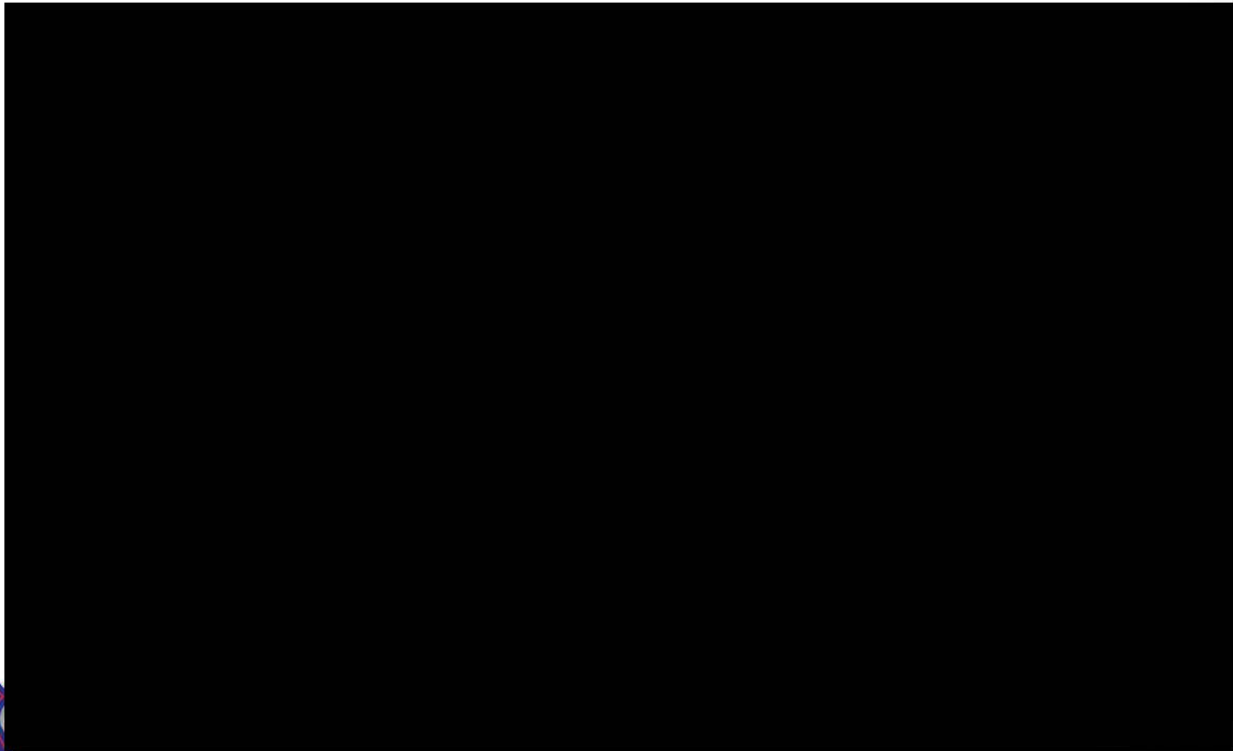
Threat #2 A Verizon Caller hates 6D



Threat #2 A Verizon Caller hates 6D



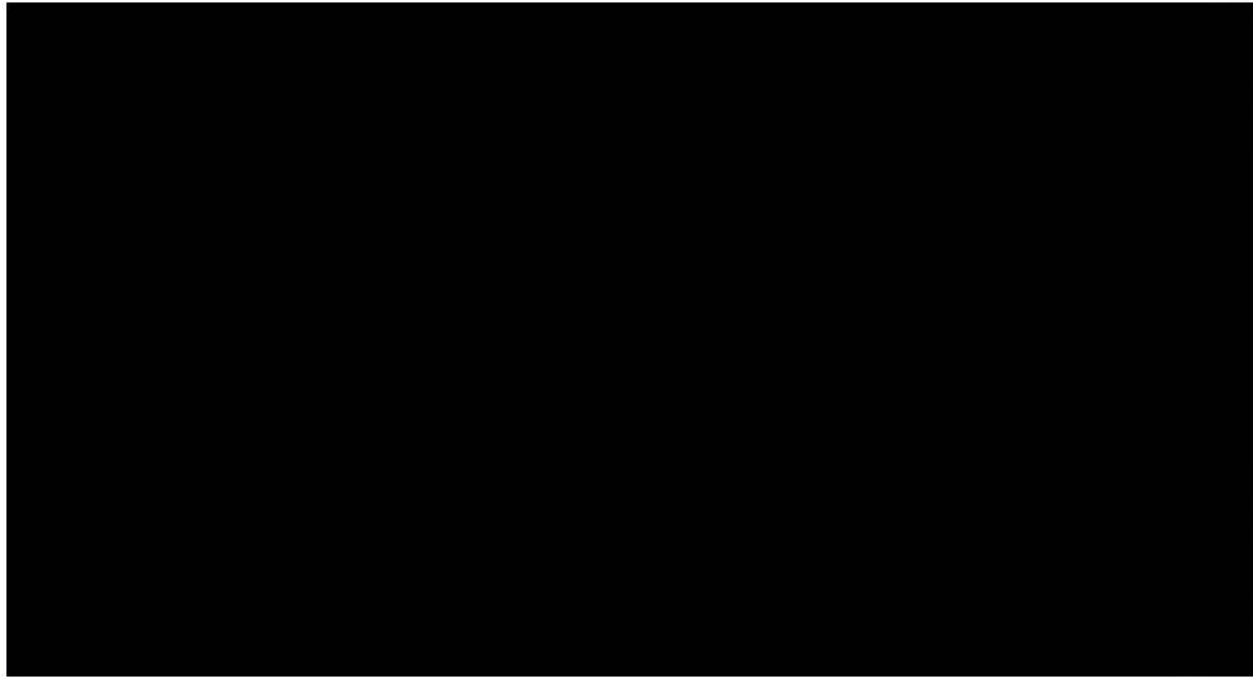
Threat #3: Twitter hates block parties



Threat #3: Twitter hates block parties

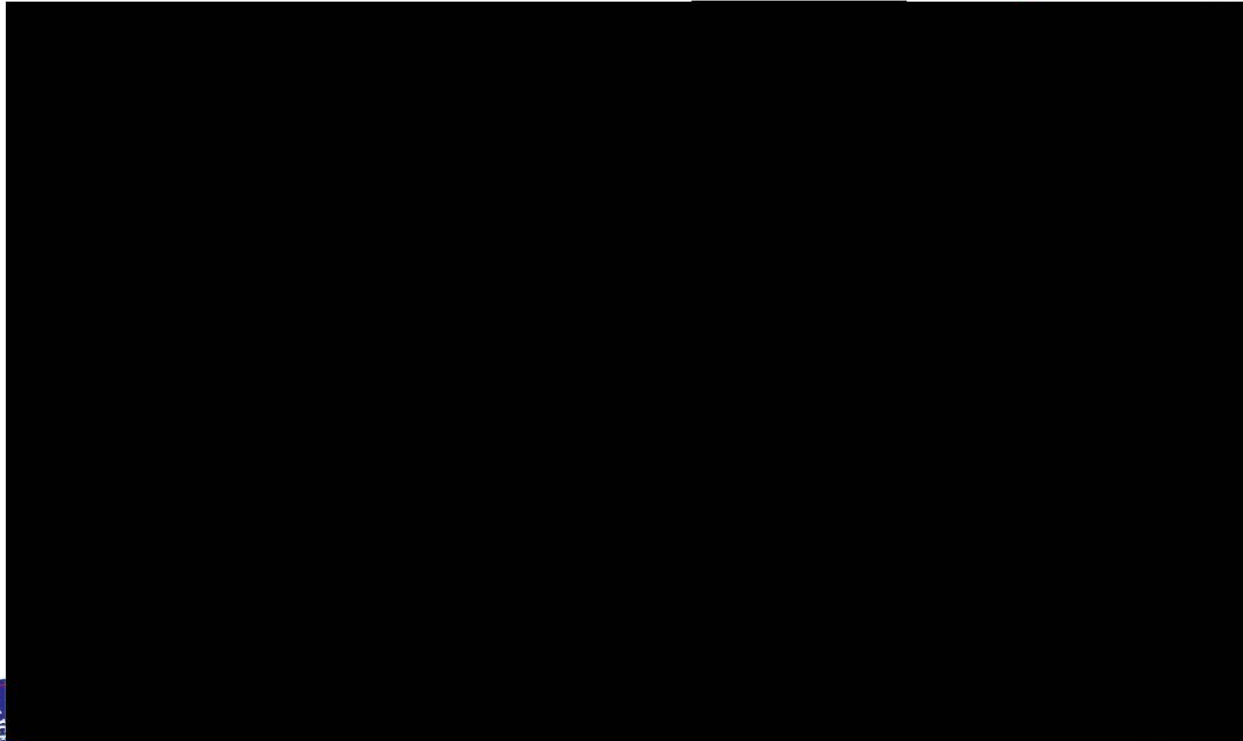


Threat #3: Twitter hates block parties



Threat #4: [REDACTED]

does not like Mondays



Threat #4: [REDACTED]

does not like Mondays:



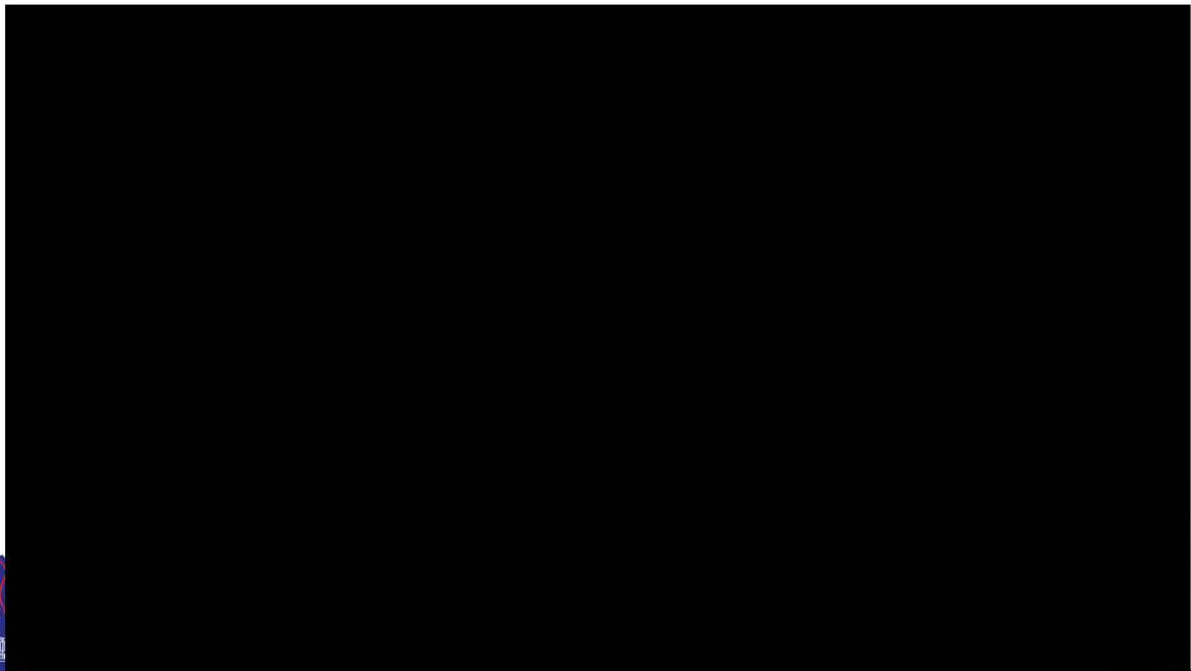
Threat #4: [REDACTED]

does not like Mondays



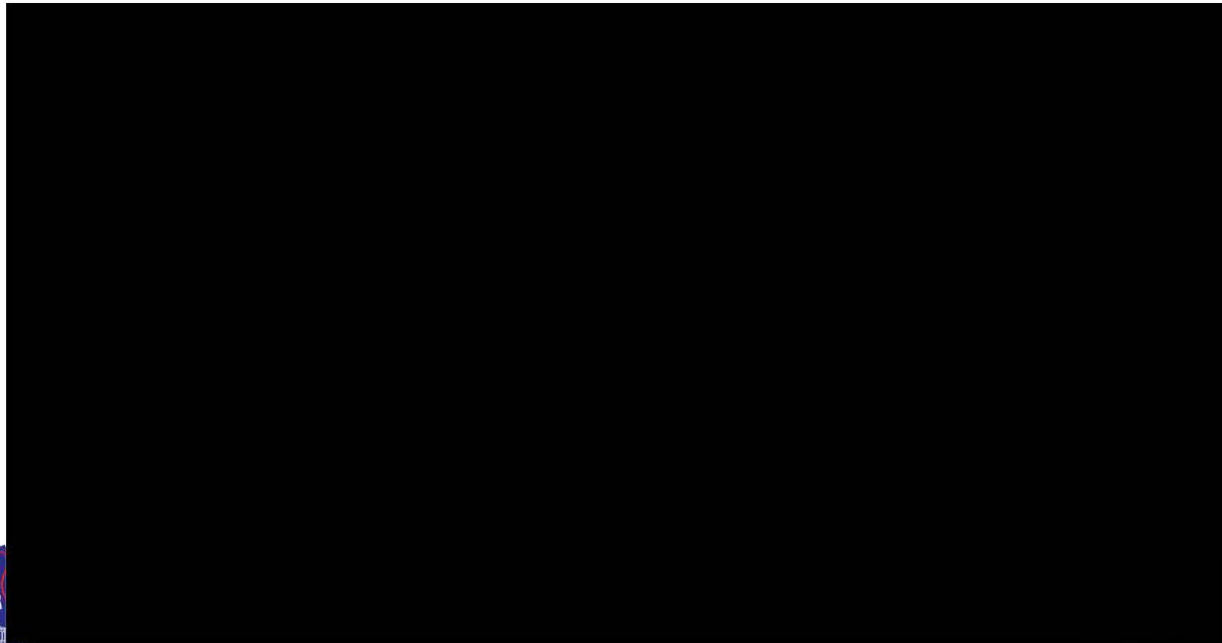
Threat #4: [REDACTED]

does not like Mondays

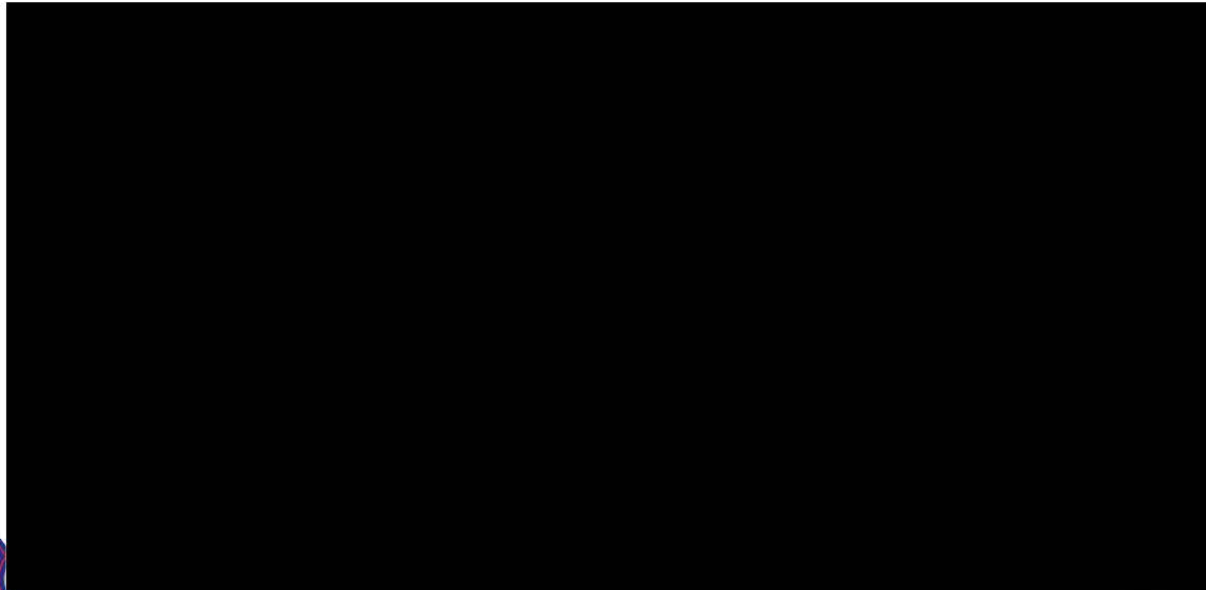


Threat #4: [REDACTED]

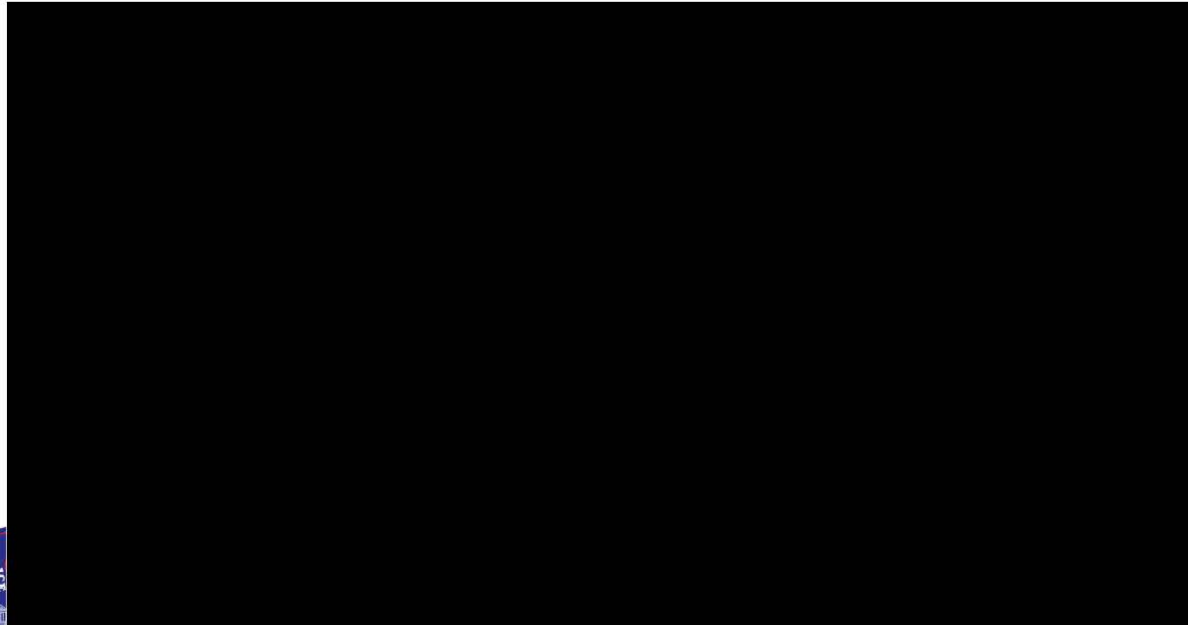
does not like Mondays



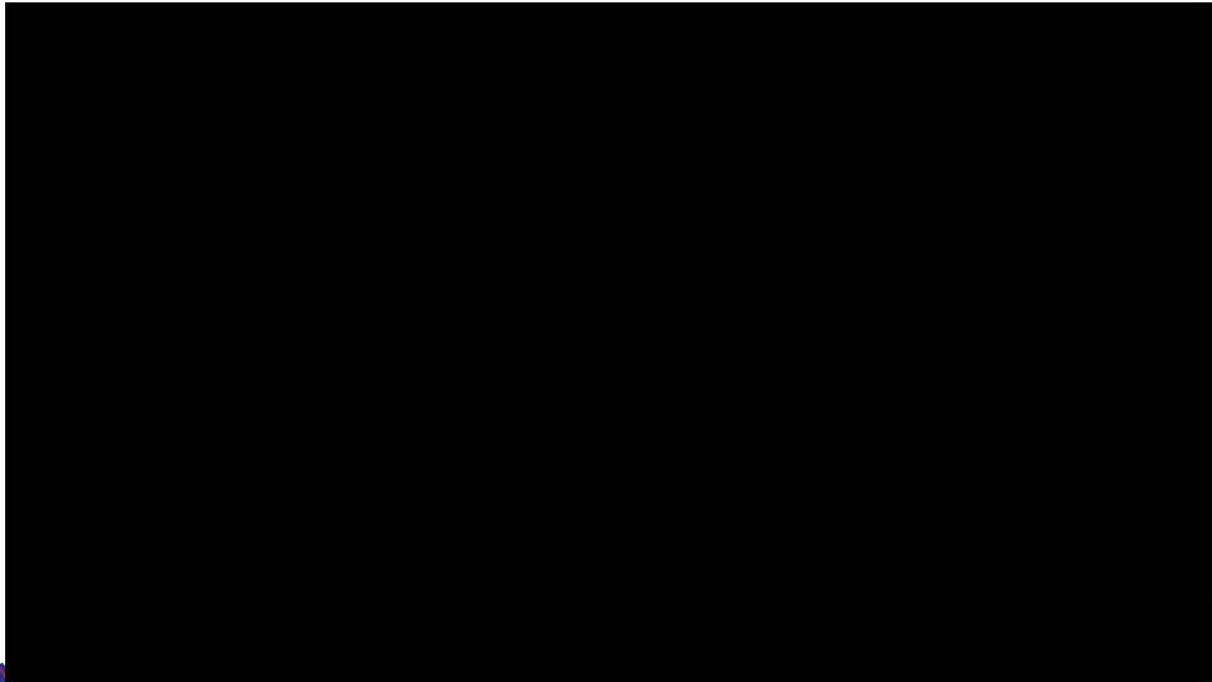
Threat #4: Jereld Fitzgerald does not like Mondays



Threat #4: Jereld Fitzgerald does not like Mondays



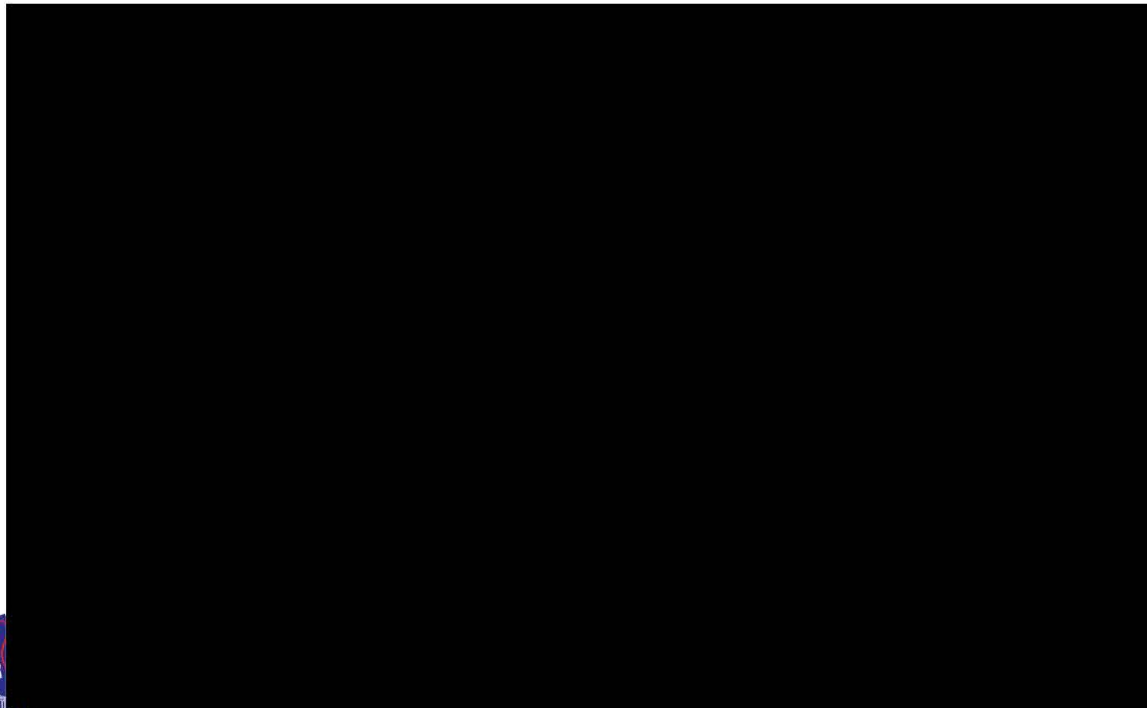
Threat #5: Craigslist Missed Connections is still a thing



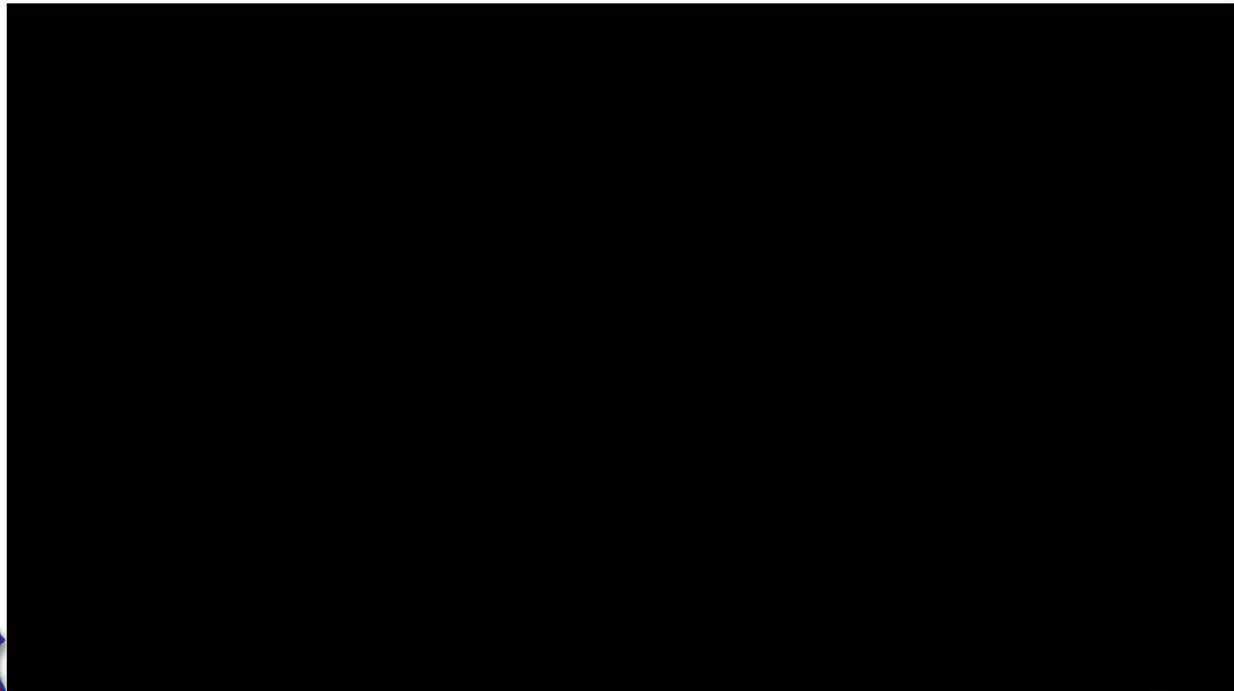
Threat #5: Craigslist Missed Connections is still a thing



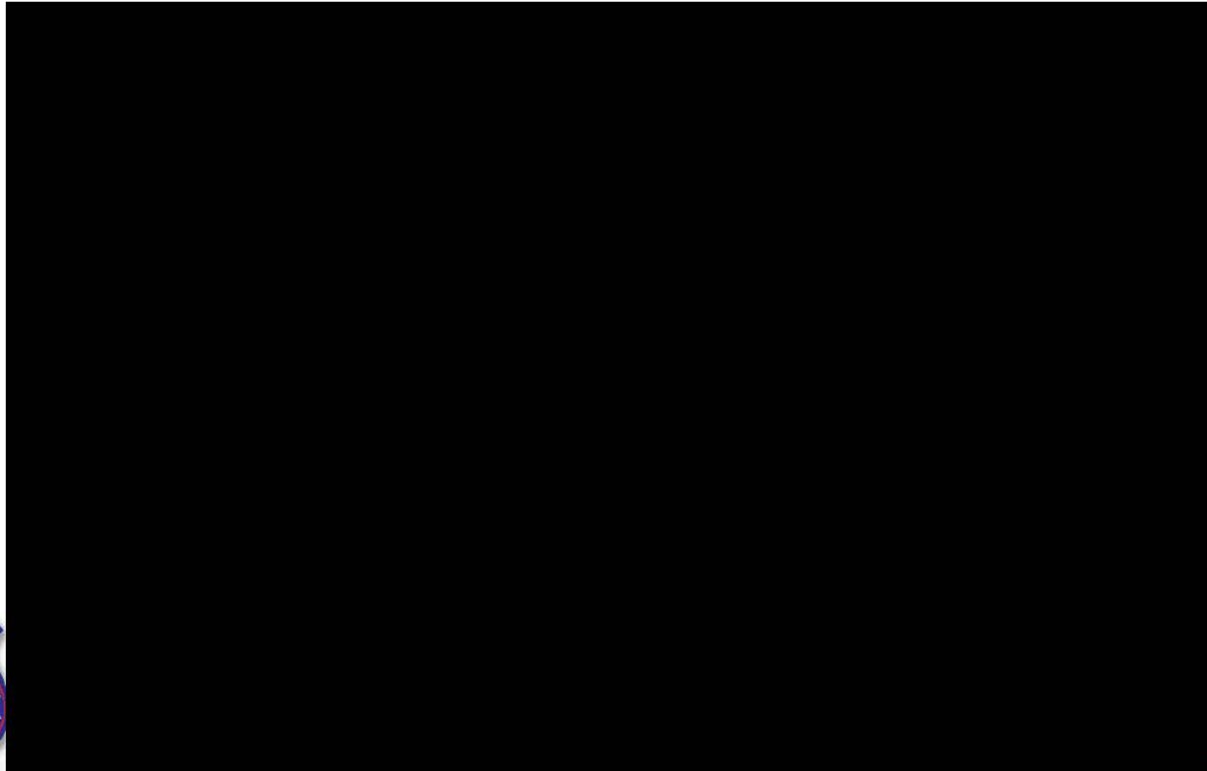
Threat #5: Craigslist Missed Connections is still a thing



Threat #5: Craigslist Missed Connections is still a thing



Threat #5: Craigslist Missed Connections is still a thing



Threat #5: Craigslist Missed Connections is still a thing



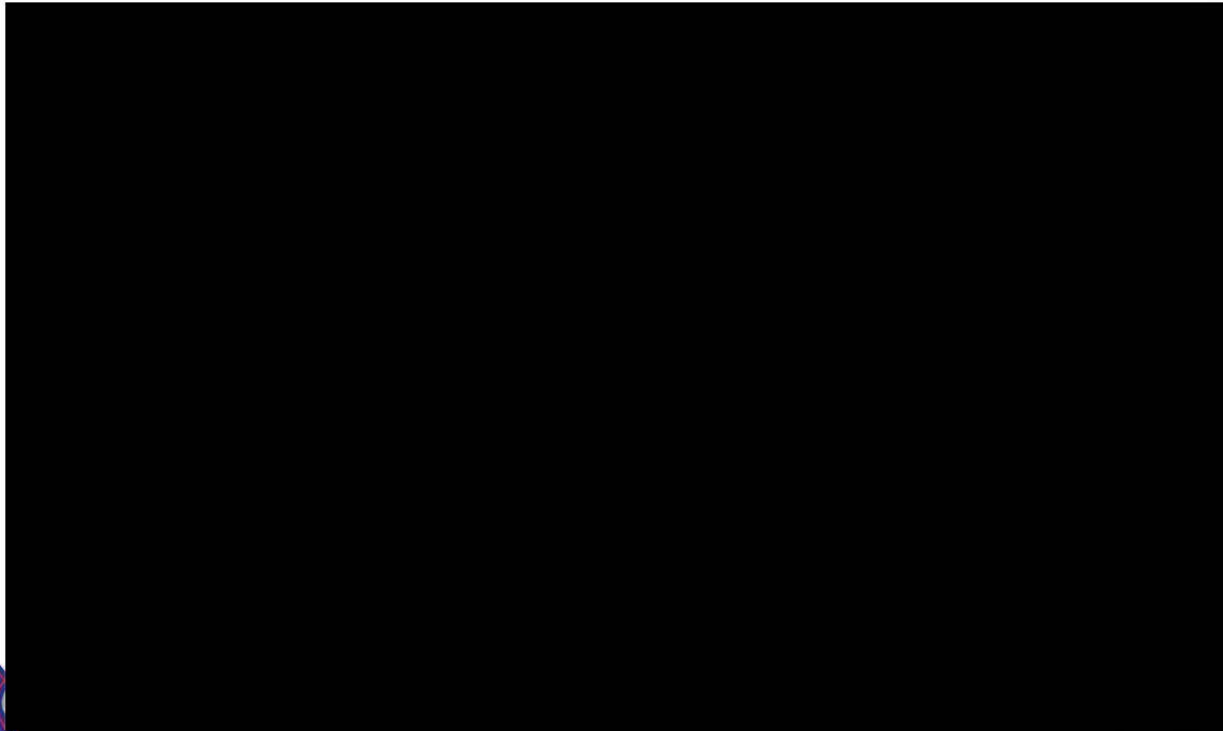
Threat #6: Chris hates Gallaudet



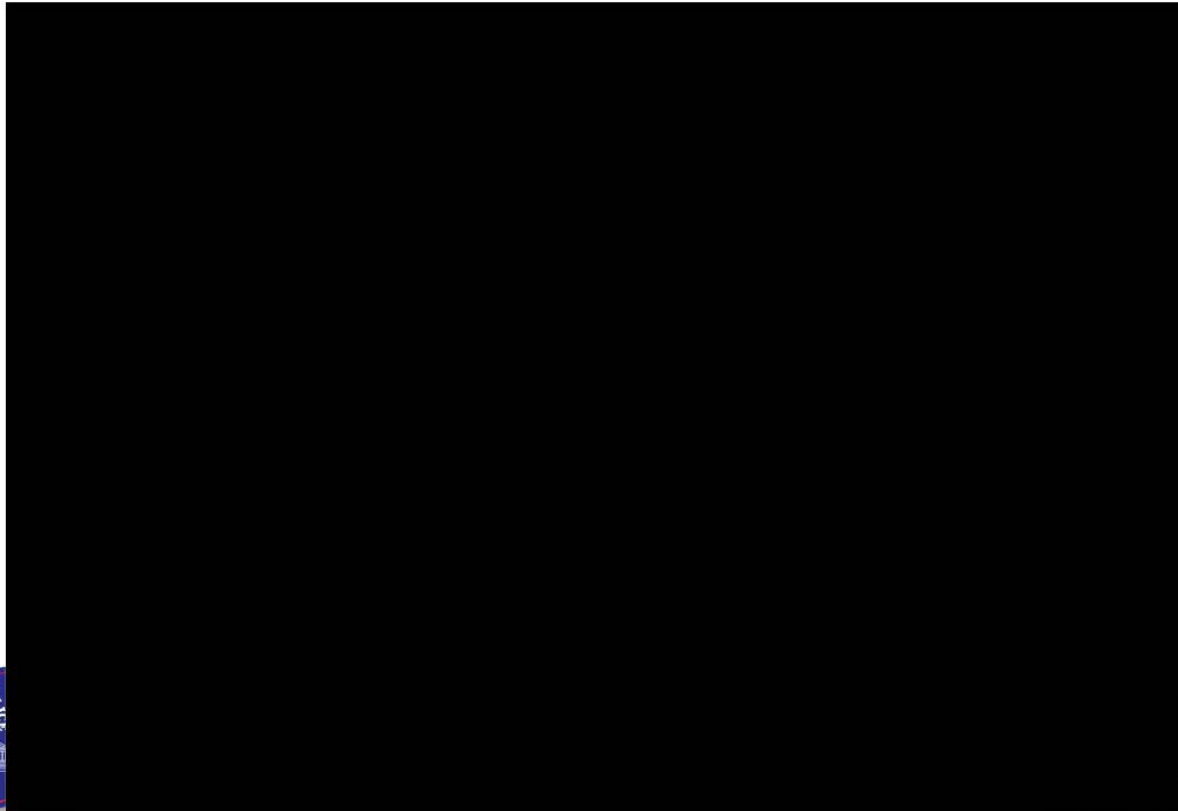
Threat #6: Chris hates Gallaudet



Threat #6: Chris hates Gallaudet



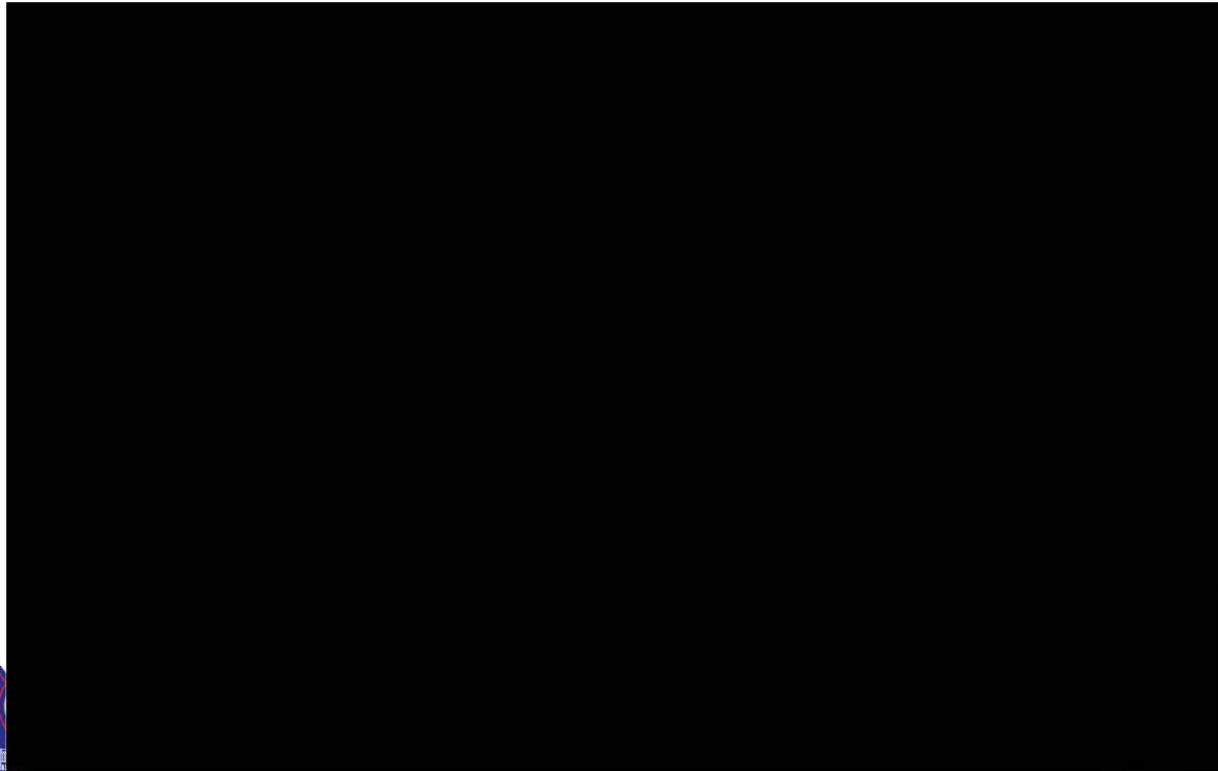
Threat #6: Chris hates Gallaudet



Threat #7: The Flash hates PlaylistLive



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



Threat #7: The Flash hates PlaylistLive:Answer 3B



Threat #7: The Flash hates PlaylistLive:Answer 3B



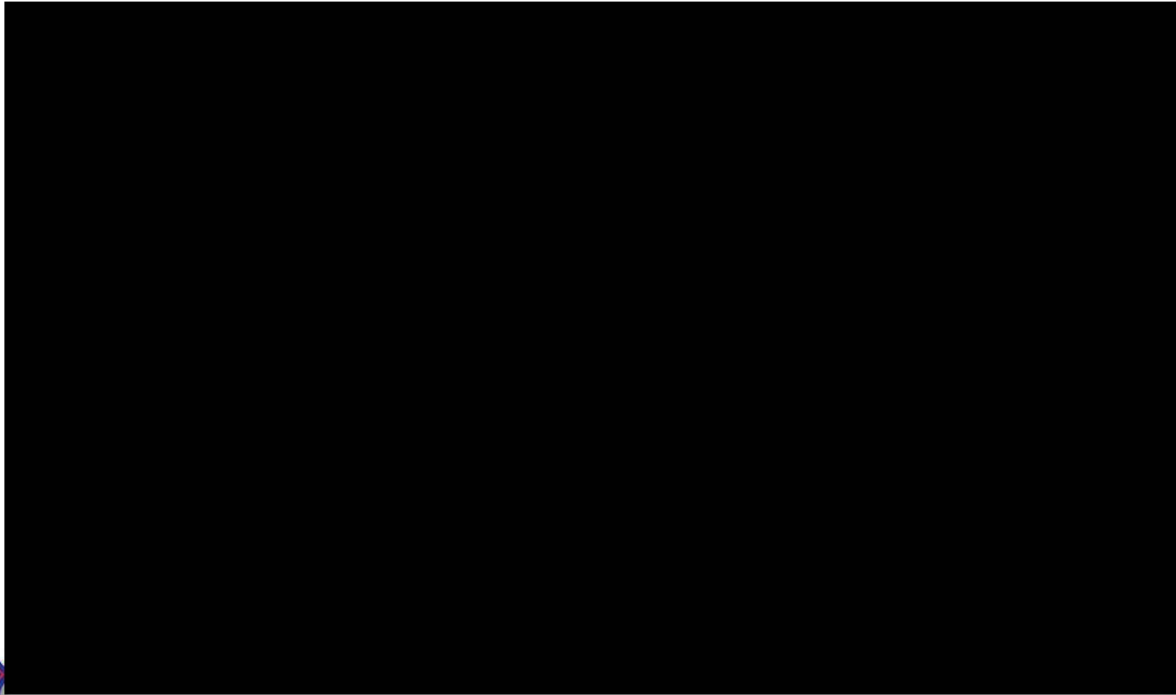
Threat #7: The Flash hates PlaylistLive:Answer 3B



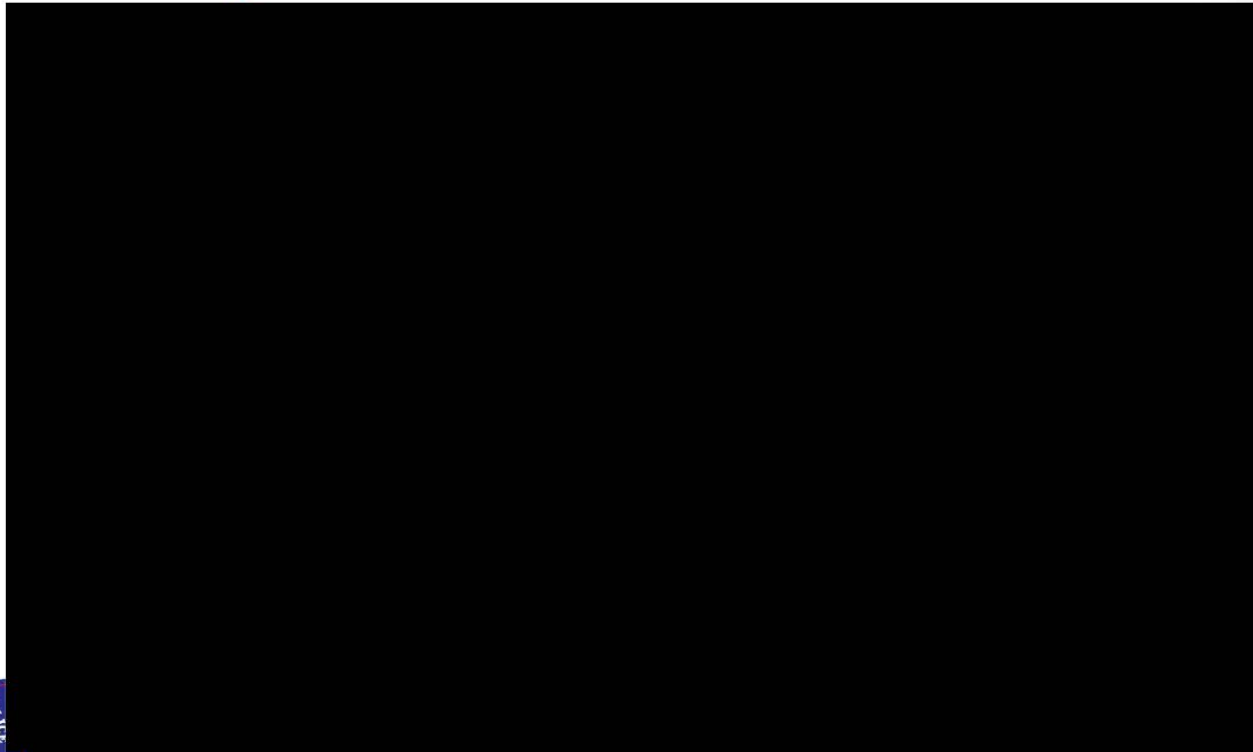
Threat #7: The Flash hates PlaylistLive: Answer 3B



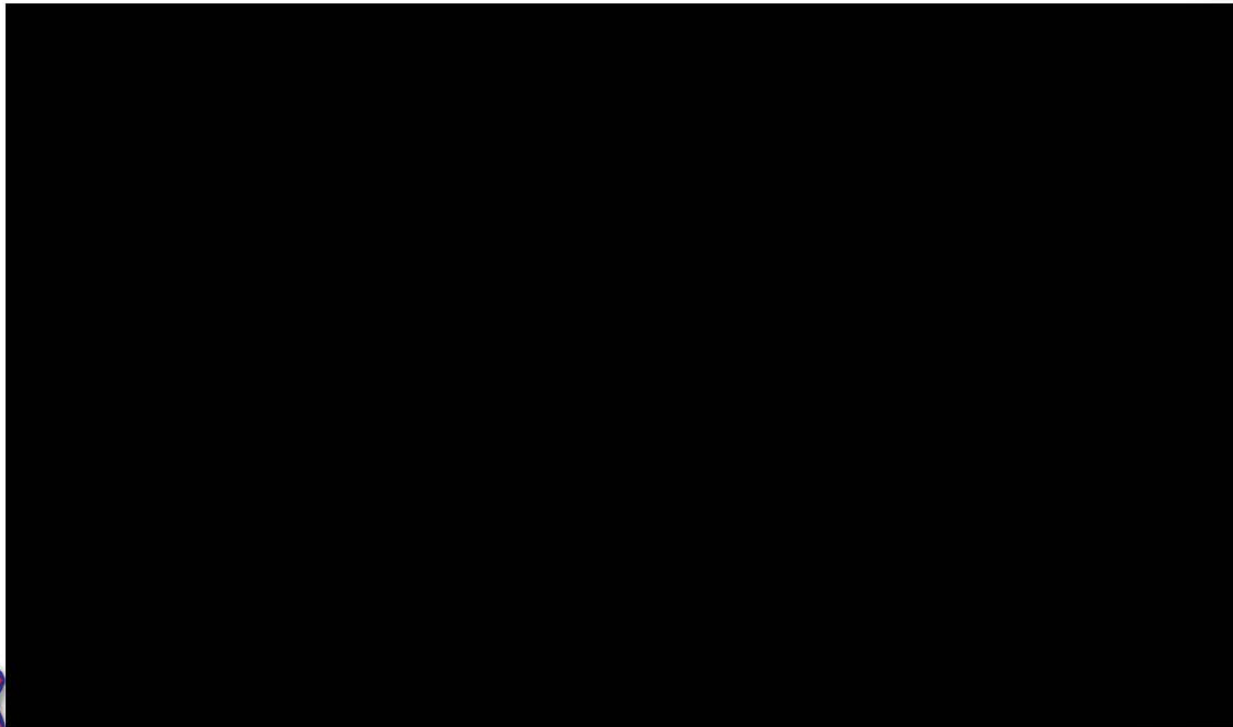
Threat #7: The Flash hates PlaylistLive: Answer 3B



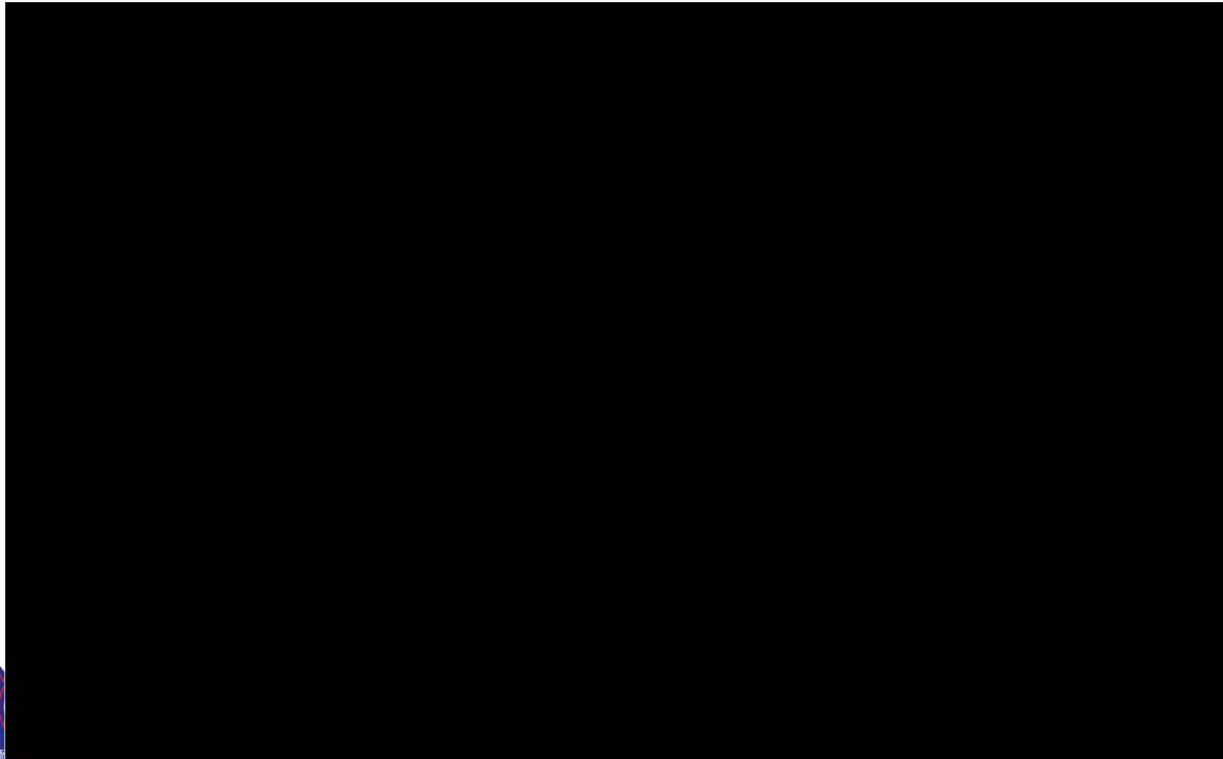
Threat #7: The Flash hates PlaylistLive: Answer 3B



Threat #7: The Flash hates PlaylistLive: Answer 3B



Threat #7: The Flash hates PlaylistLive: Answer 3B

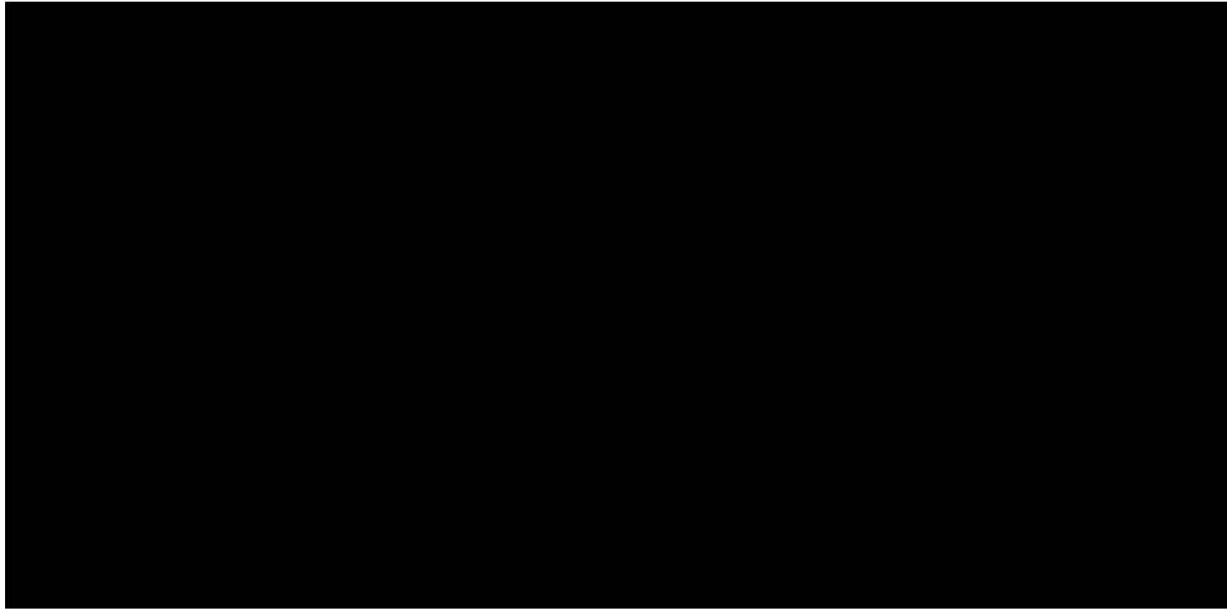


Use of Undercover Accounts

- Why create an Online Covert Account (Undercover account)?



Use of Undercover Accounts



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



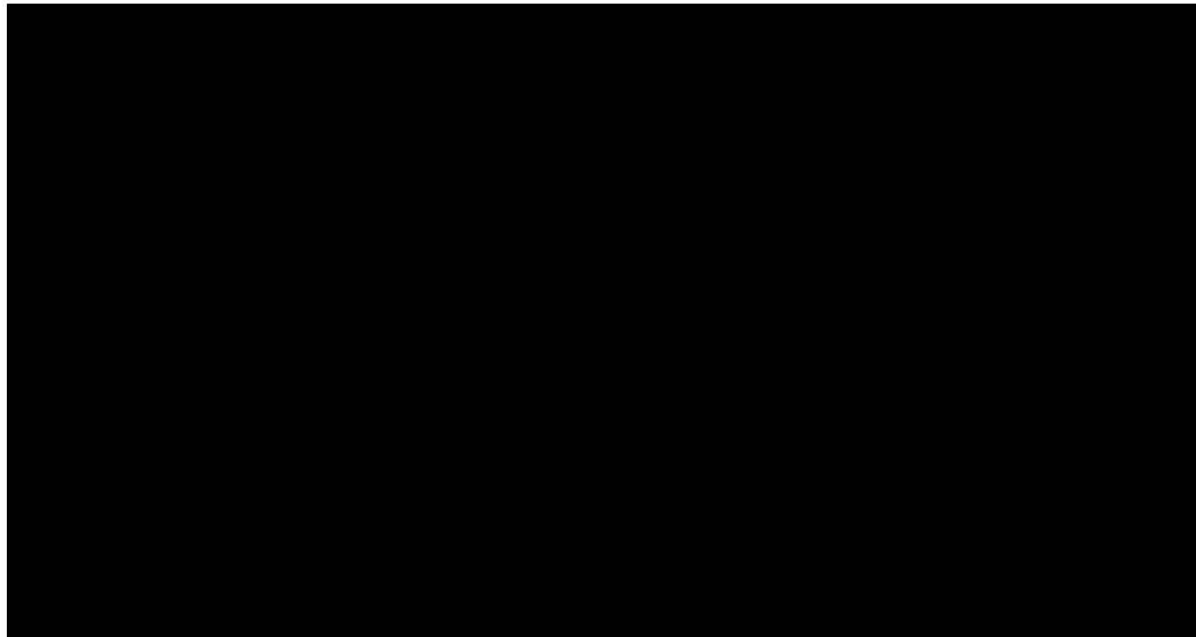
Use of Undercover Accounts



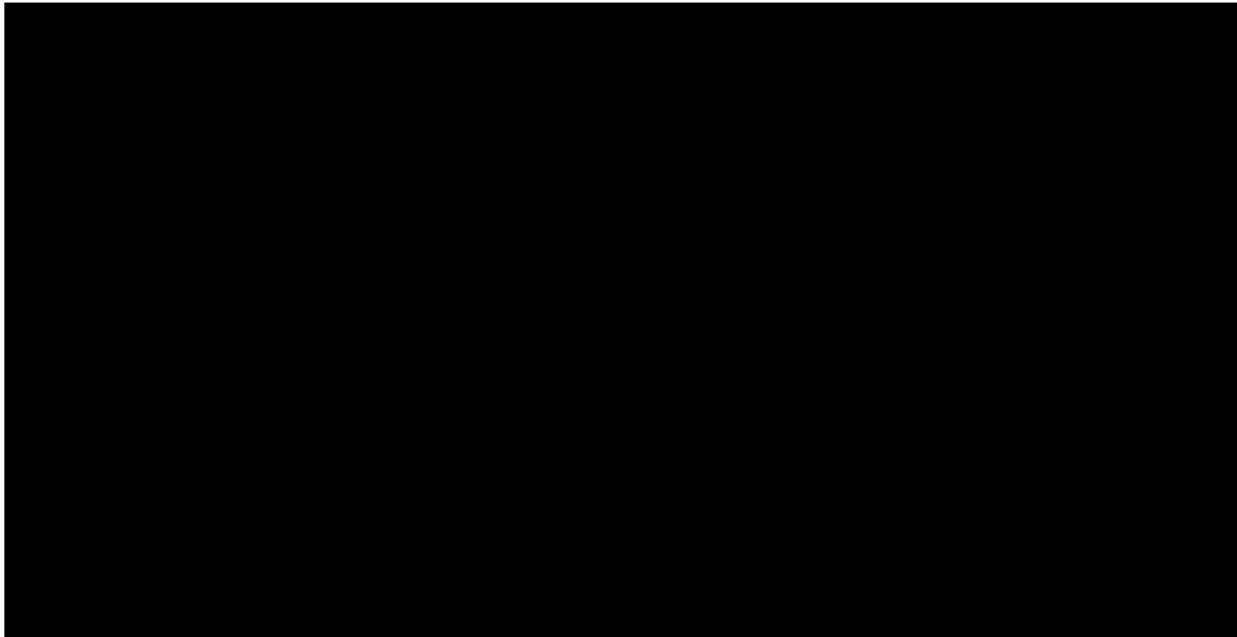
Use of Undercover Accounts



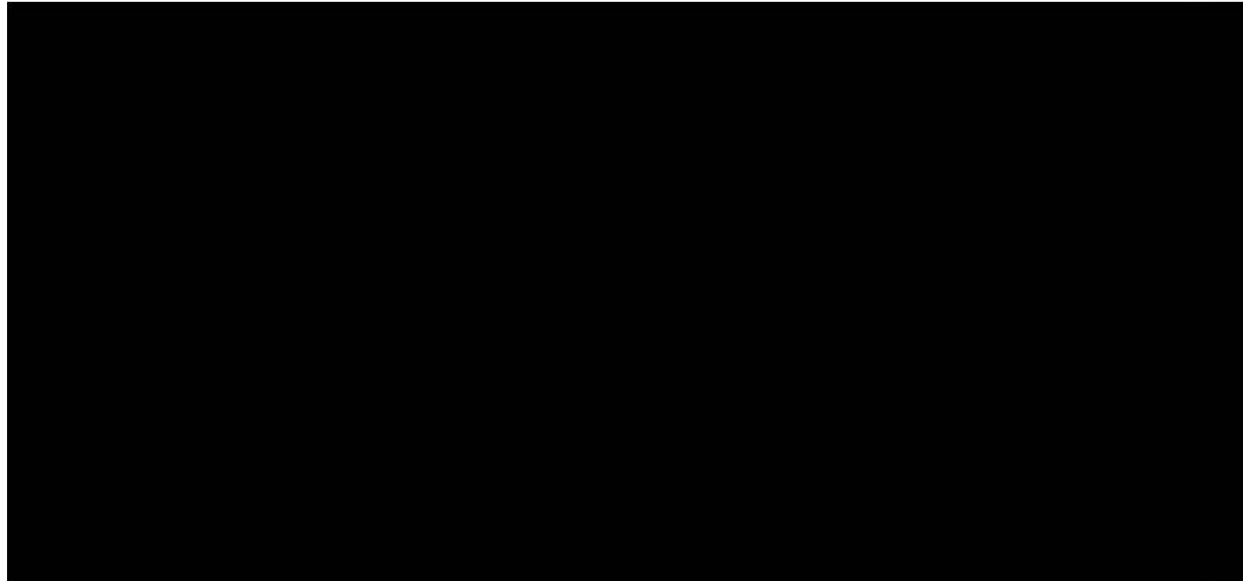
Use of Undercover Accounts



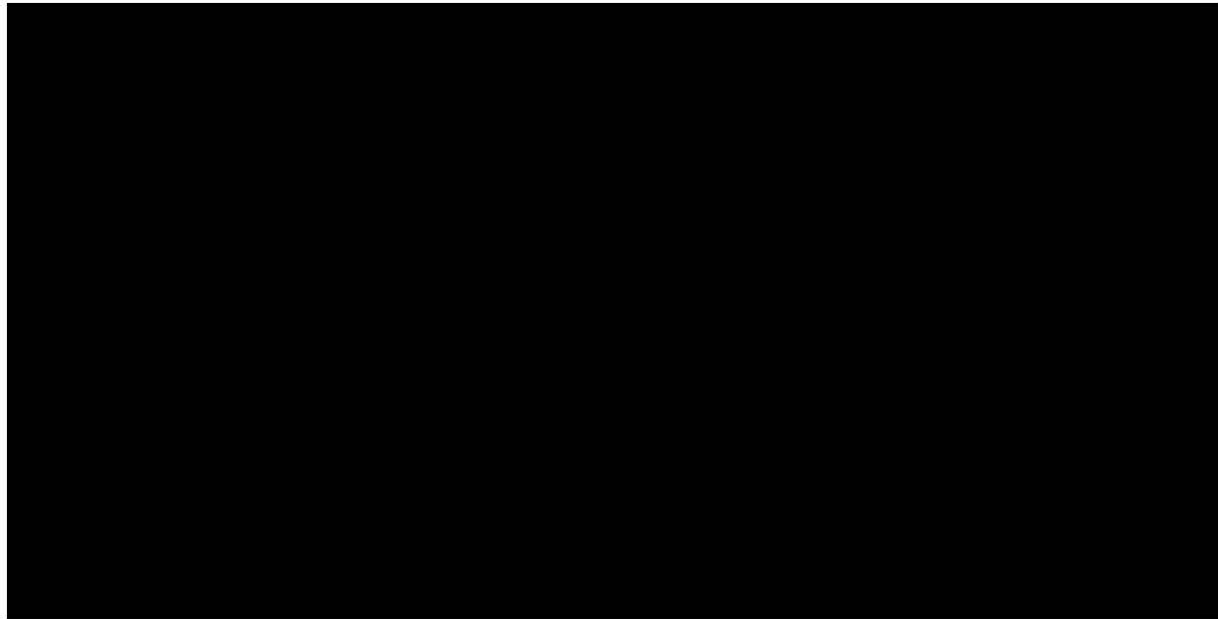
Use of Undercover Accounts



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:

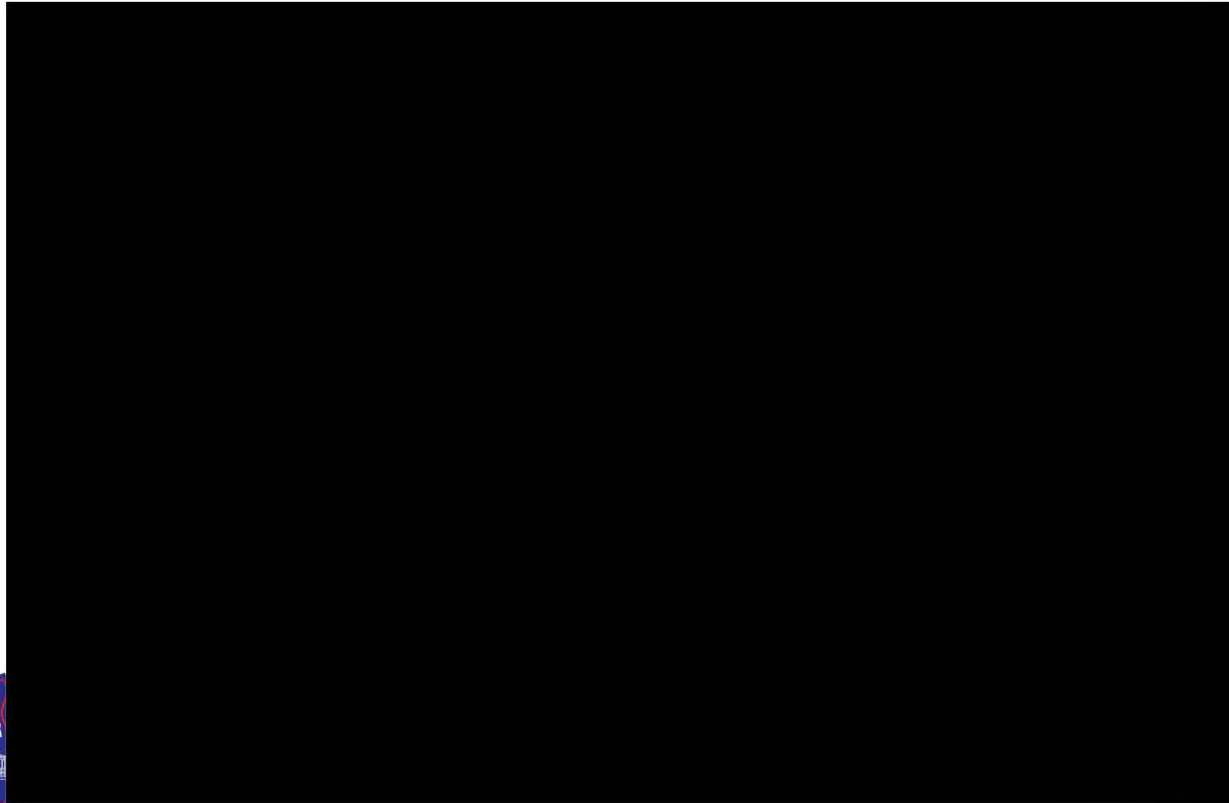
With covert Accounts, the end goal is an arrest. This may be done through an operation that introduces an Undercover or a Confidential Informant, or in the case of threats by way of a search warrant for the account.



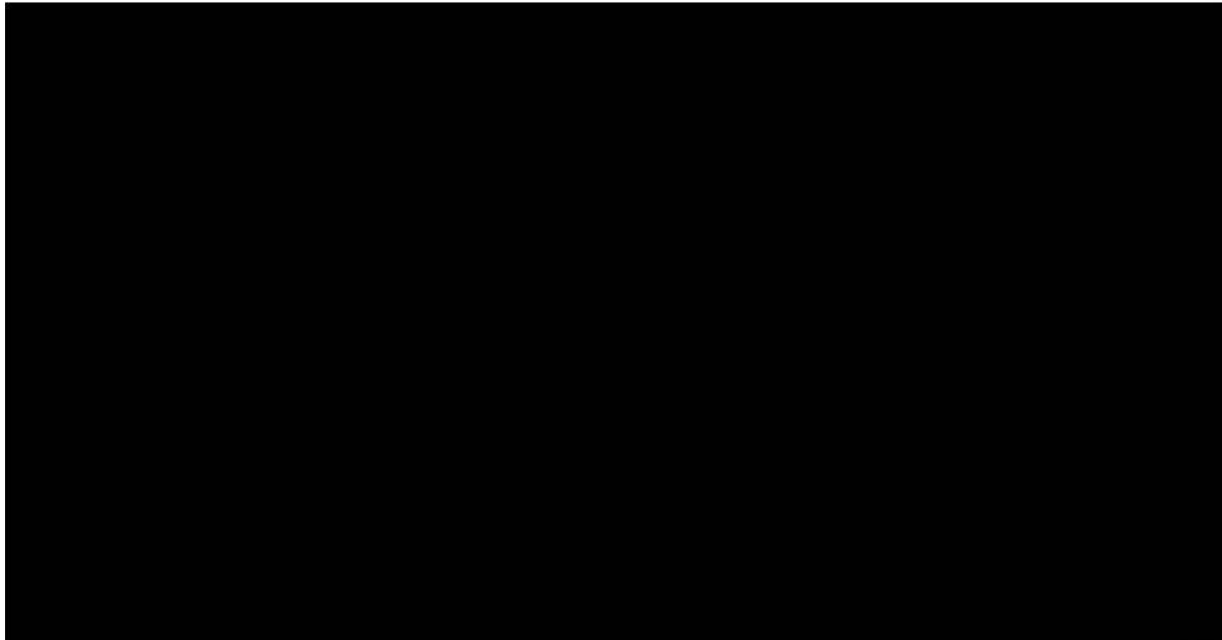
Use of Undercover Accounts



Use of Undercover Accounts



Use of Undercover Accounts



Use of Undercover Accounts



FOIA Request No.: 2021-FOIA-01634
Requester: Brennan Center for Justice

Use of Undercover Accounts



FOIA Request No.: 2021-FOIA-01634
Requester: Brennan Center for Justice

That's it, Amigos!



FOIA Request No.: 2021-FOIA-01634
Requester: Brennan Center for Justice

Exhibit B

EXECUTIVE ORDER



DISTRICT OF COLUMBIA

Subject: Social Media for Investigative and Intelligence-Gathering Purposes
Number EO-21-025
Effective Date November 8, 2021
Replaces: EO-21-024 (Social Media for Investigative and Intelligence-Gathering Purposes), Effective Date October 15, 2021
Related to: GO-OPS-304.01 (Operation and Management of Criminal Investigations)

I. PURPOSE

The purpose of this executive order is to provide Metropolitan Police Department (MPD) members with guidance on the use, management, administration, and oversight of social media for investigative and intelligence-gathering purposes.

II. PROCEDURES

A. Use of Social Media for Investigations and Intelligence-Gathering

1. Overt monitoring, searching, and collecting of information available in the public domain for any legitimate law enforcement purpose is permitted and requires no supervisory authorization. Overt use of social media in the public domain may include the use of fictitious accounts created to monitor social media provided the account is not used to engage in conversation.
2. In certain circumstances and pursuant to the procedures set forth in this order, members of the following elements may request approval to use non-official MPD social media accounts (i.e., undercover accounts) in the course of legitimate criminal investigations or intelligence collection efforts related to public safety or potential criminal activity.

Undercover Accounts
a. Criminal Investigations Division
b. Intelligence Division
c. Internal Affairs Division (criminal investigations only)
d. Narcotics and Special Investigations Division
e. Youth and Family Services Division

3. Members shall request written approval from the Narcotics and Special Investigations Division (NSID) commander through the chain of command prior to using or creating an undercover account. The NSID commander shall ensure new accounts are reviewed to ensure de-confliction with existing accounts and investigations.

4. If approved, the member may create or use an undercover social media account, profile, avatar, or a similar form of online identification.
 - a. Members shall complete training prior to using an undercover account.
 - b. Members shall not use a proprietary image or another person's likeness without prior consent.
 - c. Members using an undercover account to engage in conversations with a subject may only do so when the member is physically located in the District of Columbia (i.e., to ensure compliance with one-party consent).
 - d. Members shall not use their personal social media account or personal information to access content that is being used as part of an investigation or intelligence-gathering effort.
5. Members have no expectation of privacy when using fictitious social media accounts for overt monitoring or when using undercover social media accounts as all accounts are subject to discovery.
6. Members shall ensure that any criminal investigations involving or overlapping investigations related to First Amendment activities shall be subject to the procedures set forth in GO-HSC-801.03 (Investigations Involving First Amendment Activities).
7. Members shall use only department or federal law enforcement equipment throughout the investigation.
8. Members shall not use another individual's personal account without his or her consent and the written approval of their commanding official, the rank of commander or above.
9. Members shall not use undercover social media accounts on personal devices.
10. Members seeking to use the personal account of confidential informants or cooperating witnesses shall request specific approval from NSID through the member's commanding official.
11. Members shall not post content that is disparaging to a person or group based on race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, gender identity or expression, familial status, family responsibilities, matriculation, political affiliation, genetic information, disability, source of income, status as a victim of an intrafamily offense, place of residence or business, and status as a victim or family member of a victim of domestic violence, a sexual offense, or stalking.

12. Members shall report any potential compromise of an online alias to their official immediately upon becoming aware and be guided by his or her direction.

B. Oversight and De-Confliction

1. NSID shall provide oversight by maintaining a centralized registry of all active undercover social media accounts for de-confliction purposes. The registry shall include any assigned central complaint numbers (CCNs) or incident summary (IS) numbers, name of primary investigating member responsible for the account, date that the account was created, social media platform used to create the account, and log in credentials (i.e., username and password).
2. Commanding officials shall monitor the use of undercover social media accounts in use by their members. Commanding officials shall conduct a documented review of all accounts every 30 days to ensure:
 - a. That members are operating accounts pursuant to this order and not in a manner which could be interpreted as biased, unprofessional, or otherwise in violation of policy; and
 - b. That each investigation warrants the continued use of an undercover account.

III. DEFINITIONS

When used in this directive, the following terms shall have the meanings designated.

	Term	Definition
1.	Fictitious account	Social media identity that has been created by a member of MPD for the purpose of concealing his or her identify as a law enforcement officer in order to engage in overt monitoring of social media.
2.	Monitor	Observing social media accounts and content including sending requests to follow individual social media accounts.
3.	Post	Uploaded content or added response uploaded by another user.
4.	Profile	Information that a user provides about him or herself on a social media or similar site.
5.	Social media	Online sources that allow people to communicate, share, and exchange information with others via some form of online or cellular network platform (e.g., Facebook, Twitter, Instagram, LinkedIn). Information may include, but is not limited to, text, photographs, video, audio, and other multimedia files, message or online bulletin boards, and other similarly developed formats, to communicate with others using the same groups while also networking with other users based upon similar interests (e.g., geographical location, skills, occupation, ideology, beliefs).
6.	Undercover account	Social media identity that has been created by a member of MPD for the purpose of concealing his or her identify as a law enforcement officer in order to gain information.

A handwritten signature in black ink, appearing to read "Robert J. Contee III". The signature is fluid and cursive, with a prominent flourish at the end.

Robert J. Contee III
Chief of Police

RJC:KDO:MOC:SMM

Exhibit C



**Homeland Security Bureau
Intelligence Fusion Division**

300 Indiana Ave, NW Room 3044, Washington DC, 20001 Office: 724-4252 Fax: 202-727-5783

MEMORANDUM

TO: Criminal Intelligence Branch Members

FROM: Lieutenant Michael J. Pavlik
Criminal Intelligence Branch

DATE: April 20, 2011

SUBJECT: Operation Summer ICE Social Media Teams

As part of the Summer Crime Initiative, Operation Summer ICE, the Criminal Intelligence Branch (CIB) has been tasked with creating Social Media Teams. The mission of these teams is to monitor social media websites for possible information on criminal activity and that care is exercised so as to protect person's constitutional rights, and that matters investigated are confined to those supported by a legitimate law enforcement purpose. To that end, the following guidelines shall be followed.

Members may observe and monitor social media websites that are open to the public, with no invitation, approval or membership required. No prior approval is necessary.

Should members observe or have a reasonable suspicion that a social media website may have posts or contain information concerning criminal activity and criminal associations and such site requires an invitation, approval or membership a written request articulating such reasonable suspicion shall be submitted to the CIB lieutenant for approval prior to requesting to join or create a connection.

Members shall only monitor such websites for discussions of possible criminal activity and criminal associations and shall not engage discussions or interactions unless prior approval has been given by the CIB lieutenant.

In exigent circumstances approval maybe requested by phone followed by a written request the next business day.

Members shall print or document information only as it pertains to having reasonable suspicion of criminal activity or associations.

Approval for the above monitoring will only be approved for thirty days. Prior to the expiration members shall request a written request for an extension to the CIB lieutenant as necessary.

The CIB lieutenant shall maintain a file of all requests and shall conduct a review to determine if reasonable criminal suspicion still exists prior to the 30 day expiration.

Members shall continually monitor open pages that may have ties to known gang areas. Additionally, upon learning of a violent incident members shall query all known sites for the area that the incident occurred and any known rivals for any information that could assist in the case as well as assist in identifying any potential retaliation.

Members shall prepare a weekly report for each OSS area detailing any information gleaned. However, should a member gain information regarding any criminal acts, potential suspects, or acts of retaliation, this information shall be forwarded ASAP.

Exhibit D



**Homeland Security Bureau
Intelligence Fusion Division**

300 Indiana Ave, NW Room 3044, Washington DC, 20001 Office: 724-4252 Fax: 202-727-5783

MEMORANDUM

TO: Criminal Intelligence Branch Members

FROM: Lieutenant Michael J. Pavlik
Criminal Intelligence Branch

DATE: June 5, 2013

SUBJECT: Social Media Monitoring Policy

The Criminal Intelligence Branch (CIB) has been tasked with creating Social Media Teams. The mission of these teams is to monitor social media websites for possible information on criminal activity and that care is exercised so as to protect person's constitutional rights, and that matters investigated are confined to those supported by a legitimate law enforcement purpose. To that end, the following guidelines shall be followed.

Members may observe and monitor social media websites that are open to the public, with no invitation, approval or membership required. No prior approval is necessary.

Should members observe or have a reasonable suspicion that a social media website may have posts or contain information concerning criminal activity and criminal associations and such site requires an invitation, approval or membership a written request articulating such reasonable suspicion shall be submitted to the CIB lieutenant for approval prior to requesting to join or create a connection.

Members shall only monitor such websites for discussions of possible criminal activity and criminal associations and shall not engage discussions or interactions unless prior approval has been given by the CIB lieutenant.

In exigent circumstances approval maybe requested by phone followed by a written request the next business day.

Members shall print or document information only as it pertains to having reasonable suspicion of criminal activity or associations.

Approval for the above monitoring will only be approved for thirty days. Prior to the expiration members shall request a written request for an extension to the CIB lieutenant as necessary.

The CIB lieutenant shall maintain a file of all requests and shall conduct a review to determine if reasonable criminal suspicion still exists prior to the 30 day expiration.

Members shall continually monitor open pages that may have ties to known gang areas. Additionally, upon learning of a violent incident members shall query all known sites for the area that the incident occurred and any known rivals for any information that could assist in the case as well as assist in identifying any potential retaliation.

Members shall prepare a weekly report for each OSS area detailing any information gleaned. However, should a member gain information regarding any criminal acts, potential suspects, or acts of retaliation, this information shall be forwarded ASAP.