



EMERGENCY DISCLOSURE & PRESERVATION REQUESTS

JOINT STRATEGIC AND TACTICAL ANALYSIS COMMAND CENTER

Ms. CAROLYN MONTAGNA, DIRECTOR, JSTACC

LIEUTENANT [REDACTED] INTELLIGENCE BRANCH

METROPOLITAN POLICE DEPARTMENT

WASHINGTON, D.C.

PETER NEWSHAM
CHIEF OF POLICE

A001



- Preservation Requests
- Definition of “Exigent Circumstances”
- Emergency Disclosure Requests
 - Social Media
 - Cell Phones
 - Voice over Internet Protocol



SOCIAL MEDIA: PRESERVATION REQUEST



Many social media companies will allow for a preservation request for potentially relevant evidence in legal proceedings. The companies will preserve, but not disclose, a temporary snapshot of the relevant account records for a period of time (usually 90 days) pending service of valid legal process.

This page isn't available

The link you followed may be broken, or the page may have been removed.



[Go back to the previous page](#) · [Go to News Feed](#) · [Visit our Help Center](#)



Sorry, this page isn't available.

The link you followed may be broken, or the page may have been removed. [Go back to Instagram.](#)

Electronic Communications Privacy Act, 18 U.S.C. § 2701, et seq. (ECPA). ECPA mandates that US social media companies disclose certain user information to law enforcement only in response to specific types of legal process, including subpoenas, court orders, and search warrants

A003



- **IMPORTANT:** It is imperative to preserve social media posts immediately upon discovery. This can be done by taking a screen shot of the post, taking a picture, or capturing it on BWC. A preservation request should also be submitted for legal purposes. If the post is deleted prior to submitting the preservation request, it is gone forever.



Determine if the case involves *exigent circumstances*:

“circumstances that would cause a reasonable person to believe that relevant prompt action is necessary to prevent serious physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts”

Examples – suicidal person, kidnapping/abduction victim, person in imminent danger, at-risk missing person (mentally/physically impaired), dangerous fugitive, bomb threat or threat of mass shooting



These four facts are universally applicable for all emergency disclosure requests:

- Describe the emergency and why it poses a risk of *serious physical injury* or *death* to a specific person or group of people?
- When do you expect this emergency to take place and why do you think that it will happen at this particular time?
- What information are you seeking and how will it assist in preventing serious physical injury?
- Have you obtained or tried to obtain legal process to compel the disclosure of this data? If not, please explain why.

- Commonly used social media platforms:

- Facebook
- Instagram
- Twitter
- YouTube



Facebook and Instagram Emergency Disclosure Requests





- In 2012, Facebook purchased Instagram
- All requests for FB & IG are completed on the same site
- Account records for both platforms can be submitted during one visit to site

facebook law enforcement

All News Shopping Videos Images More Settings Tools

About 69,800,000 results (0.44 seconds)

Law Enforcement Online Request - Facebook
<https://www.facebook.com/records>

Request Secure Access to the **Law Enforcement** Online Request System ... account records solely in accordance with our terms of service and applicable law.

Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.

If you are a law enforcement agent who is authorized to gather evidence in connection with an official investigation, you may request records from Facebook through this system.

I am an authorized law enforcement agent and this is an official request

Request Access

<https://www.facebook.com/records/login/>

SOCIAL MEDIA: FACEBOOK AND INSTAGRAM



Request Access

Email [redacted]@dc.gov

Enter your email address to receive a unique link to the Law Enforcement Online Request System. The link will give you access to the system for one hour.

Fri 11/23/2018 11:08 AM
Records <records@records.facebook.com>
Access the Law Enforcement Online Requests System
To [redacted] (MPD)

The following link allows authorized law enforcement officials to securely access our Law Enforcement Online Request System. The link expires in one hour. You do not need a login or password. If you do not use this link within an hour, you must return to facebook.com/records to request a new secure link.

To access our Law Enforcement Online Request system click
<https://www.facebook.com/records/login/auth/?token=bUd3QIA1bjLLUV6bGdb-DP2lpJ8lwGtT4o1mLiAcdeDwEcGyBJcZHZ46CYHAA>
Thank you,
Law Enforcement Response Team

Facebook navigation bar with search bar and links: Home, Preservation Request, Records Request, FAQ, Log Out. The 'Preservation Request' and 'Records Request' links are circled in blue.

Law Enforcement Online Requests



SOCIAL MEDIA: FACEBOOK AND INSTAGRAM – PRESERVATION REQUEST



Requestor Information

Edit

Email [REDACTED]@dc.gov
Name [REDACTED]
Title Lieutenant, Intelligence Branch
Organization Washington, D.C. Metropolitan Police Department
Phone Number [REDACTED]
Location Washington, DC, United States



Preservation Request

Please complete all fields below to request preservation of account records. We will take steps to preserve account records in connection with official criminal investigations for 90 days pending our receipt of formal legal process. Additional information can be found in the [Facebook](#) or [Instagram](#) Law Enforcement Guidelines.

Internal Case Reference Number [?]

Accounts

Facebook

mm/dd/yyyy

Ad



Instagram user names and Facebook vanities are not permanently tied to an account and can be changed over time. In order to select the correct account, please provide the date for which you observed the activity related to your legal process.

I attest that I am a law enforcement agent authorized to request account records and all the information I have provided is accurate.

Submit

A011

SOCIAL MEDIA: FACEBOOK AND INSTAGRAM – RECORDS REQUEST



Records Request

Please complete all fields below and be sure to attach all relevant documentation. A U.S. search warrant, Mutual Legal Assistance Treaty (MLAT) or letter rogatory is generally required to compel disclosure of user content.

The Law Enforcement Response Team reviews each request separately and discloses account records solely in accordance with our terms of service and applicable law. Additional information can be found in the [Facebook](#) or [Instagram](#) Law Enforcement Guidelines.

Please note that all times are recorded in UTC and adjust your request parameters accordingly.

Internal Case Reference Number [?]

Legal Process **Select One** ▼

Nature of Case **Select a Legal Process First** ▼

Legal Process Signed Date [?]

Request Due Date [?]

Accounts **Facebook** ▼

i Instagram user names and Facebook vanities are not permanently tied to an account and can be changed over time. In order to select the correct account, please provide the date for which you observed the activity related to your legal process.

Requesting Records Between [?] **Select** ▼

| | | |
|---------------|--|--|
| Documentation | <input type="button" value="Browse..."/> | <input type="button" value="Browse..."/> |
| | <input type="button" value="Browse..."/> | <input type="button" value="Browse..."/> |
| | <input type="button" value="Browse..."/> | <input type="button" value="Browse..."/> |

Non-Disclosure Order Yes No

i A "non-disclosure order" is an order, signed by a judge that specifically prohibits Facebook from notifying the account holder at issue of the fact that Facebook has been served with legal process seeking information about their account.

I attest that I am a law enforcement agent authorized to request account records and all the information I have provided is accurate.

Internal Case Reference Number [?]

Legal Process **Select One** ▼

Nature of Case **✓ Select One** ▼

Legal Process Signed Date [?]

Request Due Date [?]

Accounts

- Subpoena
- Court Order 2703(d)
- Court Order (Other)
- Search Warrant (Domestic US)
- Pen Register/Trap and Trace
- Title III
- MLAT Search Warrant
- MLAT Court Order 2703(d)

Requesting Records Between [?]

| | | |
|---------------|--|--|
| Documentation | <input type="button" value="Browse..."/> | <input type="button" value="Browse..."/> |
| | <input type="button" value="Browse..."/> | <input type="button" value="Browse..."/> |
| | <input type="button" value="Browse..."/> | <input type="button" value="Browse..."/> |

Must be PDF, JPG, PNG or other common image formats. Please attach all relevant legal documents.

Emergency Request

By selecting Emergency Request I attest that the matter I am reporting involves imminent harm to a child or risk of death or serious physical injury to any person and requires disclosure of information without delay.

A012

SOCIAL MEDIA: FACEBOOK AND INSTAGRAM – RECORDS REQUEST



Nature of Case **Select One** ▾

Time of Threat **Select One**

Location of Threat

Age of Person at Risk

Is this related to a Live video?

Accounts

- Child Safety (Potential Harm)
- Fugitive
- Missing/Kidnapped Person
- Missing/Kidnapped/Runaway Minor
- Physical Assault
- Suicide
- Terrorist Activity
- Threats/Harassment
- Other

Requesting Records Between [?] **Select One**

Documentation

| | | | |
|--|-----------|--|-----------|
| | Browse... | | Browse... |
| | Browse... | | Browse... |
| | Browse... | | Browse... |

Must be PDF, JPG, PNG or other common image formats. Please attach all relevant legal documents.

Facebook vanities are not permanent and can be changed over time. If you are requesting records for a specific account, please provide the date of the activity related to your legal request.

i Pursuant to applicable law and our terms, we may produce data in exceptional circumstances if we have a good faith belief that your request relates to an emergency involving danger of death or serious physical injury to a person(s) and disclosure is required without delay. Answering the questions below thoroughly will help us assess whether this standard has been met. Please provide as much detail in each field as possible. We will not review requests with incomplete or insufficient information.

Describe the emergency and why it poses a risk of serious physical injury or death to a specific person or group of people.

When do you expect this emergency to take place and why do you think that it will happen at this particular time?

What information are you seeking and how will it assist in preventing serious physical injury or death?

Have you obtained or tried to obtain legal process to compel the disclosure of this data? If not, please explain why.

No Yes

SOCIAL MEDIA: FACEBOOK AND INSTAGRAM – RECORDS REQUEST



Nature of Case

Time of Threat

Location of Threat

Age of Person at Risk

Is this related to a Live video? Yes No

Accounts

i Instagram user names and Facebook vanities are not permanently tied to an account and can be changed over time. In order to select the correct account, please provide the date for which you observed the activity related to your legal process.

Requesting Records Between

| Documentation | <input type="button" value="Browse..."/> | <input type="button" value="Browse..."/> |
|----------------------|--|--|
| <input type="text"/> | <input type="button" value="Browse..."/> | <input type="button" value="Browse..."/> |
| <input type="text"/> | <input type="button" value="Browse..."/> | <input type="button" value="Browse..."/> |

Must be PDF, JPG, PNG or other common image formats. Please attach all relevant legal documents.

i Pursuant to applicable law and our terms, we may produce data in exceptional circumstances if we have a good faith belief that your request relates to an emergency involving danger of death or serious physical injury to a person(s) and disclosure is required without delay. Answering the questions below thoroughly will help us assess whether this standard has been met. Please provide as much detail in each field as possible. We will not review requests with incomplete or insufficient information.

Describe the emergency and why it poses a risk of serious physical injury or death to a specific person or group of people.

When do you expect this emergency to take place and why do you think that it will happen at this particular time?

What information are you seeking and how will it assist in preventing serious physical injury or death?

Have you obtained or tried to obtain legal process to compel the disclosure of this data? If not, please explain why.

No Yes



Twitter and Periscope Emergency Disclosure Requests





- This section applies to emergency disclosure and preservation requests for Twitter and Periscope
- In the event of an imminent threat that involves death or seriously bodily injury, law enforcement members can submit an emergency disclosure request through Twitter's Legal Request Submissions site:
 - https://legalrequests.twitter.com/forms/landing_disclaimer
- For additional information regarding law enforcement requests through Twitter:
 - <https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support#15>



SOCIAL MEDIA: TWITTER



Legal request submissions

Please confirm your identity

Welcome to Twitter's online legal request submission site. You can submit your legal request (e.g., subpoena or court order) for account information or content removal by following the steps below. We also accept emergency disclosure requests from law enforcement through this site. All non-legal requests should be submitted through our [Help Center forms](#).

If you are a law enforcement agent, government official, or other third-party intending to submit a valid legal request, please enter your full name, official email address, and confirm your authority by checking the box below. No other uses of this form are permitted.

More information is available in our [Law Enforcement Guidelines](#), [Accessing your Twitter data support article](#), and Twitter's [Privacy Policy](#).

Full name:*

Official email address:*

An email containing an authorization link to access the site will be sent to this email address.

I affirm that I have any required legal authority to submit this request and the submission is a permitted use of this system. *

Request Access



Fri 11/23/2018 11:41 AM

no-reply@twitter.com

Access link to Twitter legal request submission system

To Lamond, Shane (MPD)

Hello,

This is an automated response. Please do not reply to this email as it will not be received by our system.

We have received your request to access our online legal request submission system. Please use the following unique link to log into our secure site where you will be able to submit your legal request:

https://legalrequests.twitter.com/forms/access_disclaimer/2g87%2FBTS7KKGGWDIdbWKW154fOMHz6W0TehLj2MXQI%3D

Access via this unique link will expire on November 23, 2018 at 5:41PM UTC.

Legal Requests

Twitter Legal Request Submissions

Please select the type of request you would like to submit.

Emergency disclosure request

Submit an emergency disclosure request for account information regarding exigent situations.

Create request

Information request

Submit a request for Twitter / Periscope account information based on valid, properly scoped legal process (e.g., subpoena, warrant).

Create request

Preservation request

Submit a request for the preservation of Twitter / Periscope account information.

Create request

Removal request

Submit a request for Twitter to withhold content based on a valid, properly scoped legal request.

Create request

A017



- Name, Title, Organization, Work Email, Phone Number, Address of Work Place
- Authorizing jurisdiction is “United States – District of Columbia” (drop down menu)
- Requires internal reference number
 - Whatever helps you remember the case easily
- Can submit numerous accounts at one time
 - Require Twitter account ID(s), username(s), Periscope username(s), email address(es) and phone number(s)
- Matter type, criminal or civil
- Requested information
 - Basic account info
 - Creation date, email address and or phone number
 - Creation IP
 - Phone number
 - IP Session Logs
 - Tweets
 - Direct messages
 - Media
 - Other information
- Requested Dates
- Attach any supporting documents

SOCIAL MEDIA: TWITTER – EMERGENCY DISCLOSURE



Contact Information ?

Full name*

Title*

Organization*

E-mail*

Phone*

Fax

Street*

City*

Country*

ZIP code*

State*

Authorizing jurisdiction*

Jurisdiction authorizing your request. If the request is authorized by a U.S. Federal agency, please select "United States (Federal)".

Subject of the Emergency Investigation

Please add the account(s) and/or reported posting(s) (e.g., Tweets, Broadcasts) that are the subject of your investigation.

Reporting* Please fill out all the relevant sections and leave sections that do not apply blank. For instructions on how to find the Twitter account user ID, please refer to our [law enforcement guidelines](#).

Twitter account ID(s)

Reported account IDs of the subject account(s).

Twitter username(s)

Reported @usernames of the subject account(s). Please check the username of the account on Twitter prior to reporting and also note that account holders can change their username from time to time.

Periscope username(s)

Reported @usernames of the subject account(s). Please check the username of the account on Periscope prior to reporting and also note that account holders can change their username from time to time.

Email address(es) and Phone number(s)

Email address or phone number you believe to be associated with a Twitter account.

A019



Determining Twitter Account ID

- <http://gettwitterid.com>

Get a User's **Twitter** ID

**Please Enter a Twitter Username*

DCPoliceDept

GET USER ID



| | |
|------------------|----------------------|
| Twitter User ID: | 285198536 |
| Full Name: | DC Police Department |
| Screen Name: | DCPoliceDept |
| Total Followers: | 210,380 |
| Total Statuses: | 58,996 |



- Requires same “reporting” elements as the Preservation

Required Information

Type of emergency*

Select one type



- Requested information*
- Basic account information ?
 - IP session logs ?
 - Other information

Why this information is necessary*

Why the requested information is necessary to prevent the emergency.

Please provide any additional details

All other available details or context regarding the particular circumstances to help us better understand the situation.

Attachments

File attachments*

Please attach a screenshot of the reported content (if available).

| | |
|--|-----------|
| | Browse... |
| | Browse... |
| | Browse... |
| | Browse... |
| | Browse... |

We cannot accept individual attachments larger than 20MB.

I affirm that I have any required legal authority to submit this request and the submission is a permitted use of this system.

Select one type

- Child sexual exploitation
- Explicit content (e.g., obscenity)
- Harassment (e.g., bullying, stalking)
- Harm to minor (non-CSE)
- Missing persons / kidnapping
- National security
- Suicide/self-harm
- Threats
- Violent crime (e.g., homicide, sexual assault)
- Other



- Encompasses
 - YouTube
 - Gmail
 - Blogger
 - Chrome
 - Google....Play, Photos, Drive, Maps, Search, Voice
 - AdSense
 - Pixel Phone
 - AdWords
- Google has a LERS which sworn LE members can establish an account and can access this system at any time to submit court orders, preservation requests and/or EDs

What kinds of emergency cases?

Sometimes we voluntarily disclose user information to government agencies when we believe that doing so is necessary to prevent death or serious physical harm to someone. The law allows us to make these exceptions, such as in cases involving kidnapping or bomb threats. Emergency requests must contain a description of the emergency and an explanation of how the information requested might prevent the harm. Any information we provide in response to the request is limited to what we believe would help prevent the harm.



- **First time users need to set up a Law Enforcement Request System (LERS) account at <https://lers.google.com>**
- **Your log in for LERS will be _____@lers.google**
- **You will be required to enter a unique code upon logging in if you haven't accessed the account in the last 30 days**
 - **Have the phone linked to the account available**
- **Many times will be required to draft a letter stating the nature of the emergency and what information you are requesting**
- **Emergency Disclosure/Exigent contact number: (650) 417-9011**



Preservation Requests

- Signed & dated on MPD letterhead
- Must identify the account attempting to preserve
- Request, once processed, is valid for 90 days

Emergency Requests

- Snapchat “voluntarily discloses information when we believe in good faith that an emergency posing a threat of imminent death or serious bodily injury requires immediate disclosure of this information.”
- lawenforcement@snapchat.com

Law Enforcement Emergency Phone: + [REDACTED]

Note: This number is only for use by sworn law enforcement officials requiring emergency assistance with a threat of imminent death or bodily injury. All other inquiries from law enforcement must be directed to the email address above.

A024



Dear Custodian of Records:

I request release of records for the Snapchat account associated with _____(username, email address, or phone number) on an emergency basis pursuant to 18 U.S.C. § 2702(b)(8) and § 2702(c)(4).

I have provided below answers to the following questions in enough detail as I am able in order to provide a good-faith basis for releasing records on an emergency basis:

- What is the nature of the emergency and why does it pose a threat of imminent death or serious bodily injury that would justify immediately disclosing the requested information rather than relying on standard legal process?
- Whose death or serious bodily injury is imminently threatened?
- What specific information in our possession related to the emergency are you requesting?



EMERGENCY DISCLOSURE REQUESTS – CELL PHONES





DETERMINE THE TARGET PHONE'S PROVIDER

If you do not have a target number, attempt to get one using Accurint, TLO, or other resources.

- **Accurint/TLO:** *(If you do not have access, ask the ISS CRS for assistance)*
- **ZetX:** <https://zetx.com> → Phone Lookup
- **Fone Finder:** <http://www.fonefinder.net/>
(Free online site to determine probable wireless provider)

Once you have the probable wireless provider follow the instructions on the provided resource list, determine what information is needed.



WHAT INFORMATION DO YOU NEED?

In the case that you have a “Target Number”, you must determine what information do you need from the provider.

- Location of the phone?
 - Current location
 - Past location
 - Continuous location
- Subscriber Information?
 - Name
 - Home address



COMMON SERVICE PROVIDERS

Sprint/Nextel/Virgin/Boost: Call 1-888-877-7330 press 1

- *Call first then email request form, email will be provided by call center at the time of the request.*

Verizon Wireless: Call 1-800-451-5242 / press 9 and press 1

- *Can only get nearest cell tower which is not very accurate. Lat/Long coordinates sometimes available but is estimated*

Verizon Landline: Call 1-800-997-9981 press 9

T-Mobile/MetroPCS: Call 1-866-537-0911 press 1

- *Call first then Email request form to LER3@T-MOBILE.COM*

AT&T/Cingular/Cricket/GoPhone: Call 1-800-635-6840 then press 4

- *No forms necessary. Subscriber information will be provided immediately over the phone*

A029



RECEIVING LOCATION INFORMATION

- Most wireless providers will be able to send the location either as a one time “ping” or a periodic track received every 10, 15, or 30 minutes.
- Generally, this information can be obtained for 24-48 hours without the need of a warrant.
- **Reminder:** only the member who submits the request can obtain additional location results

Thu 7/26/2018 3:27 PM
GMPC.AT&T.Mobility.Compliance@bspfnc01.edc.cingular.net
Mobile Locator Results for 2520981

To

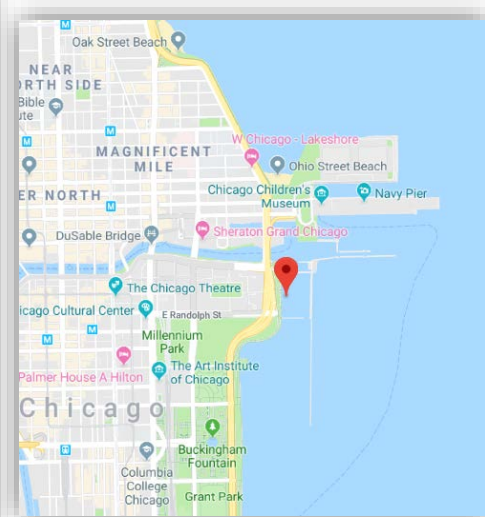
AT&T PROPRIETARY Solely for authorized persons having a need-to-know pursuant to Company instructions
AT&T CONFIDENTIAL - DO NOT FORWARD.
Initiated 2018/07/26 12:26:46 Pacific

The mobile number was located on 07/26/2018 19:26:49 GMT

| | |
|-------------------------|-------------------------------|
| ITN | 2520981 |
| Case ID | XXXXXXXXXXA111 |
| Mobile Number | XXXXXXXX2778 |
| Confidence Level | 90 |
| Longitude | W87.61235 |
| Latitude | N41.88545 |
| Radius | 592 meters (Certainty Factor) |
| Data Source | 4G-GMPC |

If the data source on your email indicates 4G, these results are presented in decimal format. 3G and Historical results are in DMS (Degrees, Minutes, Seconds format). Depending on your mapping system, you may need to convert these results for accurate mapping.

The results provided are AT&T's best estimate of the location of the target number. Please exercise caution in using these records for investigative purposes as location data is sourced from various databases which may cause location results to be less than exact.



Voice over Internet Protocol (VoIP), is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular phone line.

Because a number is a VoIP number and NOT a cellular telephone number, there is no pingable/GPS or cell site location information native to the number itself. However, the last time the number has been used will likely link back to a specific IP address that may be able to be traced.

Some companies sell VoIP numbers in bulk to other companies. Two common companies are:

- Bandwidth
- Inteliquent/Onvoy





VOICE OVER INTERNET PROTOCOL (VOIP)

Bandwidth: <https://www.bandwidth.com/legal/law-enforcement-guide/>

- All exigent requests must be made in writing via email, as Bandwidth does not provide customer of record information based only on a verbal request.
- Send an email to: uslawenforcement@bandwidth.com
- Include the target number, your law enforcement agency name, your contact information, and indicate in the subject line of your email that you have an exigent situation.
- Bandwidth will respond back via reply email with customer of record information promptly after assessing the request.

Inteliquent: <https://www.inteliquent.com/contact-legal/contact-for-exigent-circumstances>

- Fill out requested information on the above website and then call 800-933-1224, Option 2.

Onvoy: <http://www.onvoy.com/legal/law-enforcement-support>

- For after-hours emergency situations, please contact their Network Operation Center (“NOC”) at 1-800-933-1224, Option 2. The NOC is able to process and respond to after-hours emergency requests.
- An emergency disclosure form will be emailed to you (use MPDCIC@dc.gov)
- Fill out form and send it back.

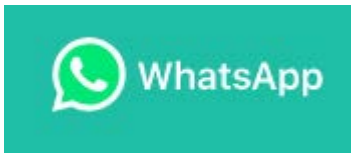
Once the information has been received from these companies, you’ll likely have to put in an Emergency Disclosure with another company.

VOICE OVER INTERNET PROTOCOL (VOIP)



Below are some secondary companies that may have IP addresses that belong to Bandwidth or Inteliquent. Many of these companies have “Apps” you can download on your phone.

- WhatsApp: <https://faq.whatsapp.com/en/general/26000050>
 - Download Emergency Disclosure Form: <https://www.whatsapp.com/legal/WhatsApp-Emergency-Disclosure-Request---For-Official-Use-Only.pdf>
 - Fill out the form and send to records@whatsapp.com (with the subject line of “Emergency”)
- Text Now: <https://supportfree.textnow.com/hc/en-us/articles/206318775-Law-Enforcement-Emergency-Disclosure-Process>
 - See link for Emergency Disclosure Process: www.textnow.com/lawenforcement
 - Email lawenforcement@textnow.com (with the subject line "Emergency Disclosure Request") ← fastest
 - Call 202-888-4004



VOICE OVER INTERNET PROTOCOL (VOIP)



Once you receive an IP address, you'll need to find out the Internet Service Provider (ISP):

- <https://whatismyipaddress.com>
- <https://www.ultratools.com/tools/ipWhoisLookup>

Some common ISPs:

- **AT&T:** call the National Compliance Center (NCC) at 800-635-6840, Option 4
- **Comcast Xfinity:** <https://www.xfinity.com/~media/403eed5ae6f46118ddbc5f8bc436030>
- **Charter Communications/Time Warner/Spectrum:** <https://www.spectrum.com/policies/lea.html>
- **Verizon FIOS:** call the Law Enforcement Resource Team (LERT) at 800-451-5242, Option 4 (<https://info.publicintelligence.net/VerizonLawEnforcementResourceTeam.pdf>)

When in doubt, Google the name of the ISP with either “law enforcement” or “emergency disclosure”.

Subscriber Information

- Name
- Home address
- Phone number
- Email address
- Last login



- The following website can be used to obtain contact information to submit Emergency Disclosure Requests and legal process to many social media sites and Internet service providers:
- <https://www.search.org/resources/isp-list/>

The screenshot shows the website <https://www.search.org/resources/isp-list/>. The page features the SEARCH logo and a navigation menu with links for Home, About Us, Membership, Solutions, Resources, Blogs, and Get Help. The main content area includes a paragraph explaining the ISP List as a law enforcement community effort and another paragraph offering assistance through the Assistance & Training Center. A search bar is present with the text "Select an ISP from the drop-down menu to access contact information:" and a dropdown menu currently displaying "ISP Quick Search". A right-hand sidebar lists various resources, including Publications & Templates, Surveys, Podcasts and Webinars, **ISP List**, SEARCH Investigative and Forensic Toolbar, Repository QA and Cost Analysis Tools, IT Security Self- & Risk-Assessment Tool, Public Safety Project Resources, High-Tech Crime Investigative Resources, and Information Sharing Resources. At the bottom right, there is a callout box stating: "An additional resource for ISP contact information is the [Library of Congress' Directory of Service Provider Agents](#)".



- **Most telephone calls made to 9-1-1 contain Automatic Numbering Information/Automatic Location Information (ANI/ALI)**
- **Automatic Numbering Information with a 911 area code prefix indicates that the cell phone used to make the 9-1-1 call is not active, and the 7-digit phone number after the area code is seven digits of the phone's Electronic Serial Number (ESN), Mobile Equipment ID (MEID), or International Mobile Equipment Identity (IMEI)**
- **Deactivated cell phones are usually untraceable as they cannot be "pinged" or called back**
- **Automatic Location Information may provide GPS location of device in that instant; however, you cannot get updated location information on the phone unless caller places another 9-1-1 call**



- **Although Emergency Disclosure Requests can be used to obtain information quickly in emergency situations, you should always follow up with proper legal process (subpoena or search warrant)**
 - **Any EDR information used as evidence in a criminal case without a follow up subpoena or search warrant may be ruled inadmissible, e.g. cell phone content, social media posts**
- **NOTE: Most social media companies will disclose to the user that a preservation request, emergency disclosure request, or search warrant for subscriber information has been submitted unless a court order requiring nondisclosure is obtained.**

QUESTIONS?



METROPOLITAN POLICE DEPARTMENT

300 INDIANA AVENUE NW – WASHINGTON, DC – 20001 – 202.727.9099

WWW.MPDC.DC.GOV

Totals

| | |
|--|---------|
| Total Crime | 276,891 |
| All Violent Crime | 41,527 |
|  Homicide | 1,140 |
|  Sex Abuse | 2,217 |
|  Assault w/Dangerous Weapon | 16,213 |
|  Robbery | 21,957 |
| All Property Crime | 235,364 |
|  Burglary | 16,842 |
|  Theft f/Auto | 85,642 |
|  Theft/Other | 111,197 |
|  Motor Vehicle Theft | 21,567 |
|  Arson | 116 |



Criminal Research Specialist – Social Media Use Policy

The Criminal Research Specialists will only utilize social media to seek or retain information that:

1. Is based upon a criminal predicate or threat to public safety; or
2. Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
3. Is useful in crime analysis or situational assessment reports for the administration of criminal justice and public safety.

The Criminal Research Specialist staff shall not use their own personal accounts to perform any searches via social media. Instead, they will use the specified CRS accounts to search publicly available information via social media sites. There shall be absolutely no interaction between the CRS personnel and the subject/group. The accounts shall be used solely for monitoring and viewing “open” profiles. The CRS staff will not try to “friend”, “follow”, “like”, “post”, etc. on any of the subjects’ pages or information. Any violation of this policy is a direct violation of MPD Policy and will result in disciplinary action.

Additionally, the CRS staff will not change or alter the CRS social media accounts in any way unless instructed to do so by the CRS Supervisor. The CRS accounts shall not be used for any purposes that are not work-related.

After a major incident (such as a homicide or shooting), the CRS personnel shall try to obtain information in reference to the victim’s or suspect’s social media accounts. Any information found in these accounts shall be relayed to the detective in a Preliminary Investigative Report.

The method behind finding any information found via social media must be documented properly in the report. For example:

- The following information was obtained from Accurint’s “Virtual Identity Report”.
- The following information was obtained by searching the phone number xxx-xxx-xxxx through the Facebook search function.

Additionally, if an individual is found by searching any of their known associates, the source individual must be noted.

If social media has been found, the website links and relevant screenshots must be sent to the detective. It is ultimately the job of the detective to determine accuracy, validity, and/or authenticity of the information. Information obtained by the CRS via social media may not be submitted as evidence. The detective must subpoena the information for it to be admitted to court. Social media postings should not be disseminated to outside agencies, unless approved by the CRS Supervisor.

Section 1: Minimum social media requirements**Section 2: Taking social media results and searches a step further****Section 3: Negative social media results**

- All ISS usernames and passwords for social media searches are saved in the Social Media folder as “CRS Social Media Passwords.doc”
- Access links to various online resources and internet search tools in the document saved as “ISS Online Resources” in the Social Media folder.
- Additional social media search tips are located in the document “Social Media Search Techniques” in the Social Media folder.

Section 1:

At a minimum, the following procedures are required to uncover social media profiles:

1. Query various name combinations, phone numbers, and email addresses for the subject through the following sites:
 - a. **Facebook, Google, and at least two other search engines** from the ISS Online Resources document.
2. Access Accurint
 - a. Query the subject in Accurint’s Virtual Identity Report.
 - i. Click on all URLs provided in the Virtual Identity Report that are associated to the subject.
 - b. If the subject is a juvenile or no information is returned in public records, also search for relatives and/or current address(es) of that subject through Accurint and/or TLO to find a relative that resides at the subject’s address.
 - i. If a social media profile is obtained for a relative (mother, father, sibling), thoroughly search the profile (friends list, about section, posts, etc.) in an effort to locate a profile for the individual of interest.
 1. The document “**Social Media Search Techniques**” saved in the Social Media folder provides guidance on searching private social media profiles.
 - c. If no profile can be found for the individual of interest, include the relative’s social media profile and URL in the report.

Section 2:

If a profile is uncovered, the following procedures are required:

1. If a social media account is uncovered, the URL handle as well as the name/alias provided on the social media account should be searched in **Google, Facebook, Instagram, Twitter, YouTube, and at least one additional** site that has a username search in an effort to uncover additional profiles.

Use the following template to document positive search results. Plug in or take out what parameters were searched in the italicized portion of the template. This information should appear in the beginning of the social media section.

POSITIVE results

- I conducted searches based on the parameters available on each site using the [arrestee, person of interest, decedent, etc] name(s), DOB(s), SSN(s), email(s), phone(s) and other various identifiers. The following systems returned results that appear to be relevant: [list websites accessed here]

If profiles are found, the following template should be used in the body of the social media section of the report for every social media site that produced results, as seen below:

- I conducted [website] searches based on [search parameters] and received the following results:
Facebook URL: <https://www.facebook.com/CRS>
**Insert screenshots of any relevant timeline, about section, photos, etc.
 - I conducted [website] searches based on [search parameters] and received the following results:
Instagram URL: <https://www.instagram.com/CRS>
**Insert screenshots of the about section, photos, etc.
2. If a photo or video is posted on a social media account where firearms or ammunition is viewable; the account URL, image URL, and screenshot of the image in which a firearm is shown **must be emailed** to the following GRU and Intel members: Cmdr. John Haines, Lt. [REDACTED], Sgt. [REDACTED], and Lt. [REDACTED].

If photos on social media reveal firearms or ammunition; the following template should be used under the website URL:

- The account URL, image URL, and screenshot of the image in which a firearm is shown was sent on [DATE] to GRU and Intel for situational awareness.

Section 3:

If no profile is uncovered, the following procedures are required:

1. Access TLO, as TLO tends to provide more phone numbers and email addresses tied to search results. Include or exclude this information in the report based on your judgment as not all information is accurate.
2. If searches have been exhausted, and no relevant social media information has been found; see below on how to document negative results.

In the Possible Social Media section, use the following template to document negative search results. Plug in or take out what parameters were searched in the italicized portion of the template. This information should appear after any positive results or in the beginning of the social media section if no results are returned.

NEGATIVE results

- I conducted searches based on the parameters available on each site using the [arrestee, person of interest, decedent, etc] *name(s), DOB(s), SSN(s), email(s), phone(s)* and other various identifiers. The following systems yielded negative or unrelated results: [list websites accessed here]



SOCIAL MEDIA

INVESTIGATIVE SUPPORT SECTION
JOINT STRATEGIC & TACTICAL ANALYSIS COMMAND CENTER

METROPOLITAN POLICE DEPARTMENT

WASHINGTON, D.C.

PETER NEWSHAM
CHIEF OF POLICE

A043

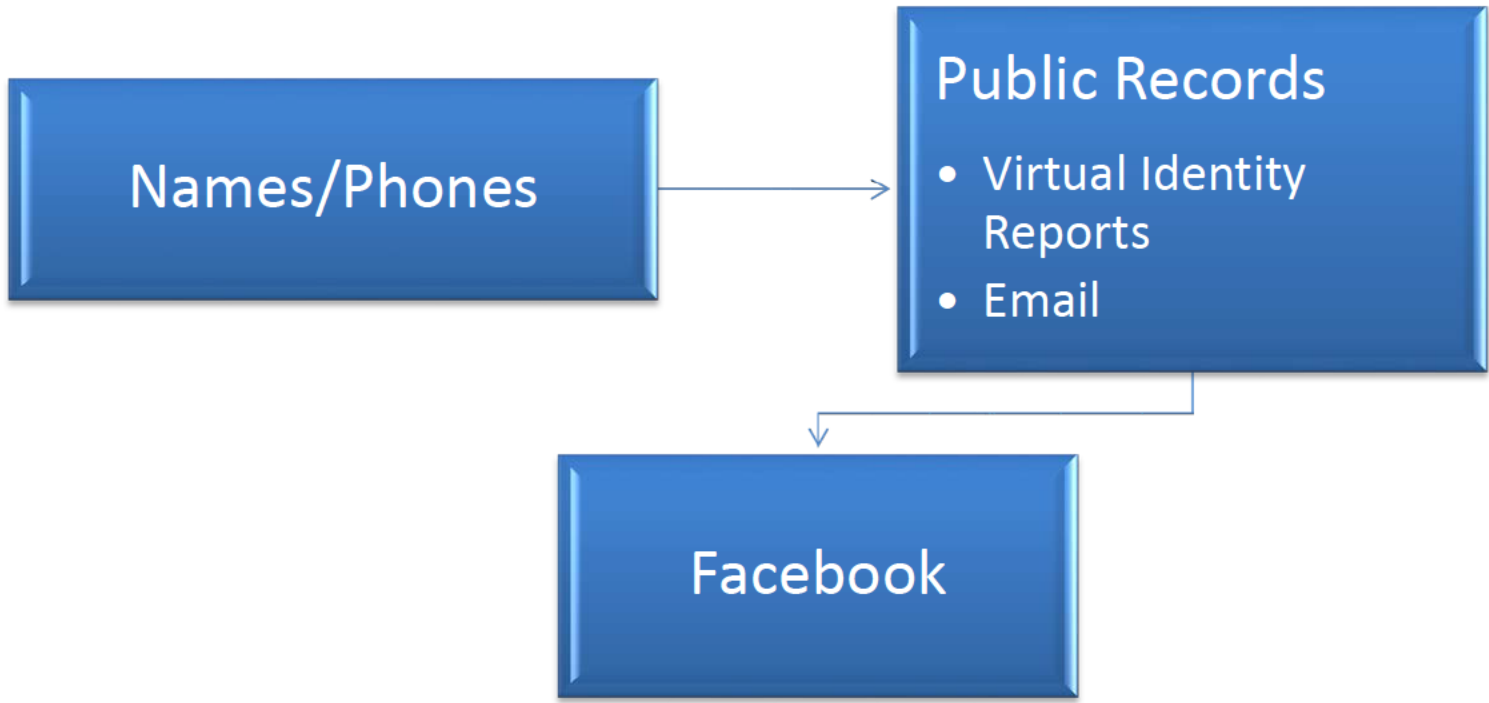


- Provide insight on how the Investigative Support Section (ISS) provides open source intelligence for investigative purposes
 - Old vs New procedures
- Techniques
- Challenges & Solutions
- Examples/Success stories



- Gaining actionable intelligence off social media about a subject
 - Weapons, narcotics, active areas, chatter, #hashtags, friends, activities, family members, etc.
- More targeted searches
- Ability to search a variety of social networking sites, but often use the most popular at the present time (Instagram, Twitter, Facebook, Youtube, Google)
- Search public profiles, pictures, blogs, comments, etc.





Barely scratching the surface



Robbery Arrestee:



Accurint:

Virtual Identity Report



Facebook:



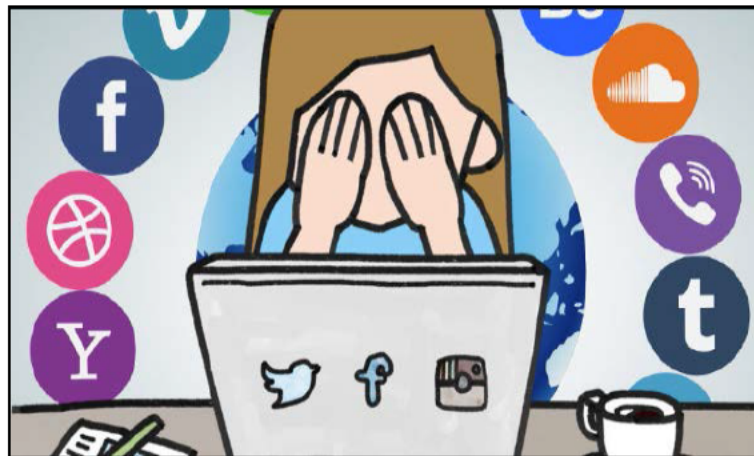
We couldn't find anything for [redacted]

Looking for people or posts? Try entering a name, location, or different words.

**SOME THINGS THAT
ARE TRUE ARE NOT
VERY USEFUL**

SOCIAL MEDIA: CHALLENGES

- Time
 - ✓ SOLUTION
 - New social media protocol
 - In-depth searches post major incident
- Changing Usernames
 - ✓ SOLUTION
 - Variations of their previous usernames, check associates profiles for tagged photos
- Private Accounts
 - ✓ SOLUTION
 - Known associates and family members sharing tagged photos
- Getting Blocked
 - ✓ SOLUTION
 - Change username, view profiles publicly
 - Storiesig.com
- Search Restrictions
 - ✓ SOLUTION
 - Specialized search sites (Spokeo, Pipl, Webstagram, Facebook Messenger)





Name(s), Phone(s),
Email(s), Various Identifiers



Accurant Virtual Identity Report, Facebook,
Google and at least 2 other search
engines/sites



If Profile is uncovered:

- URL handle, alias names queried through Google, Facebook, Instagram, Twitter, YouTube, and at least one additional site

Additional steps if no
profiles found

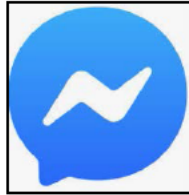


Use other public records (TLO) to find any
possible emails, phones, relatives, etc.



If searches are exhausted, document all sites
searched. Revisit if homicide/major case of
interest

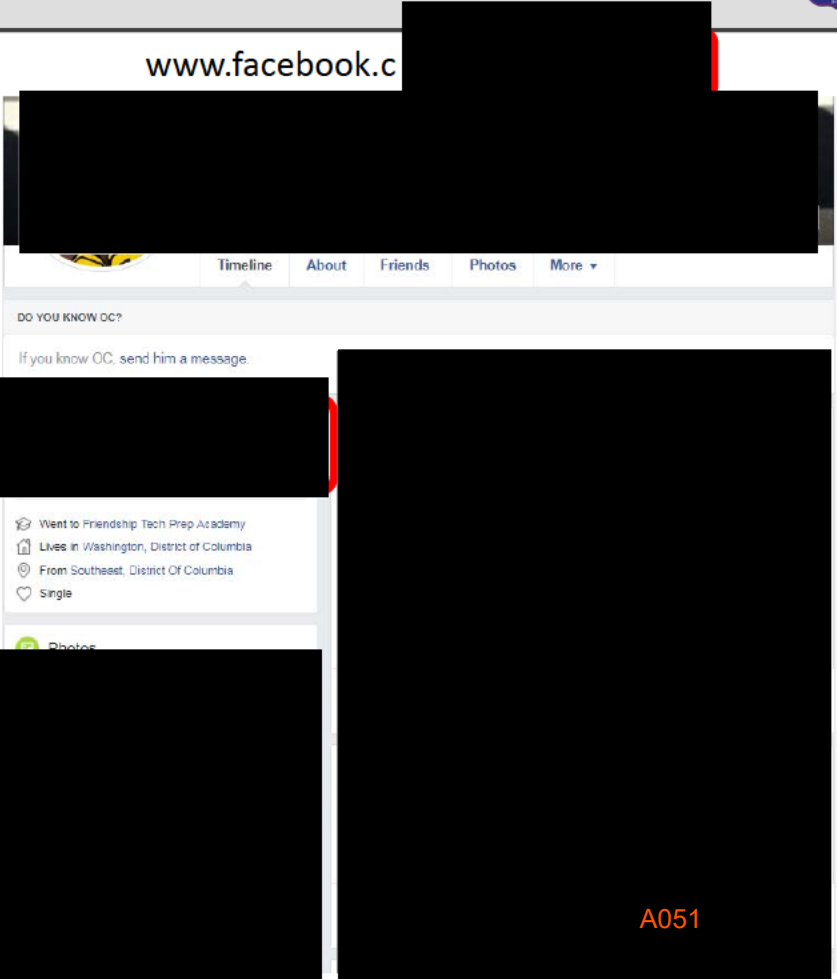
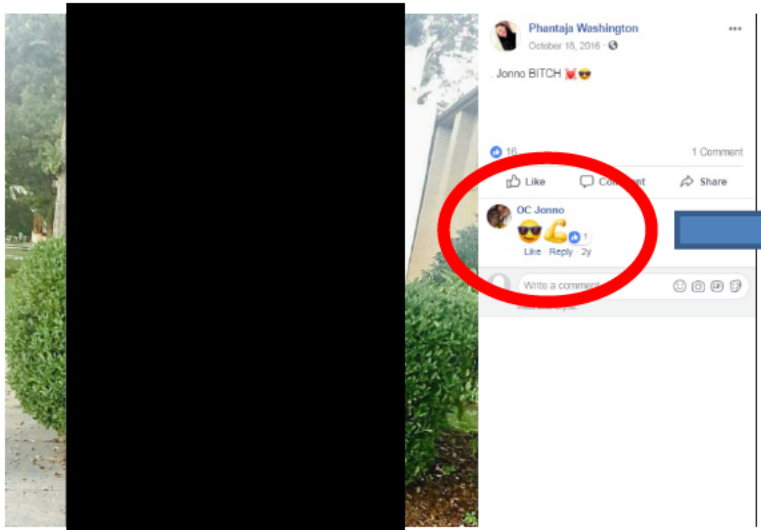
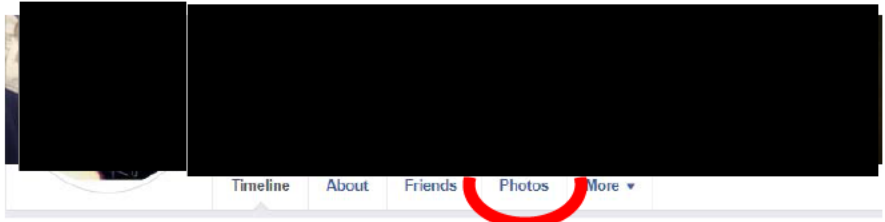
SOCIAL MEDIA: RESOURCES



FACEBOOK



- Exhausted searches on armed robbery arrestee, Daejon Ross. Found mother's Facebook account; however, no links to her son.
- Next, Daejon Ross ex-girlfriend/child in common: Phantaja Washington



A051



www.instagram.co

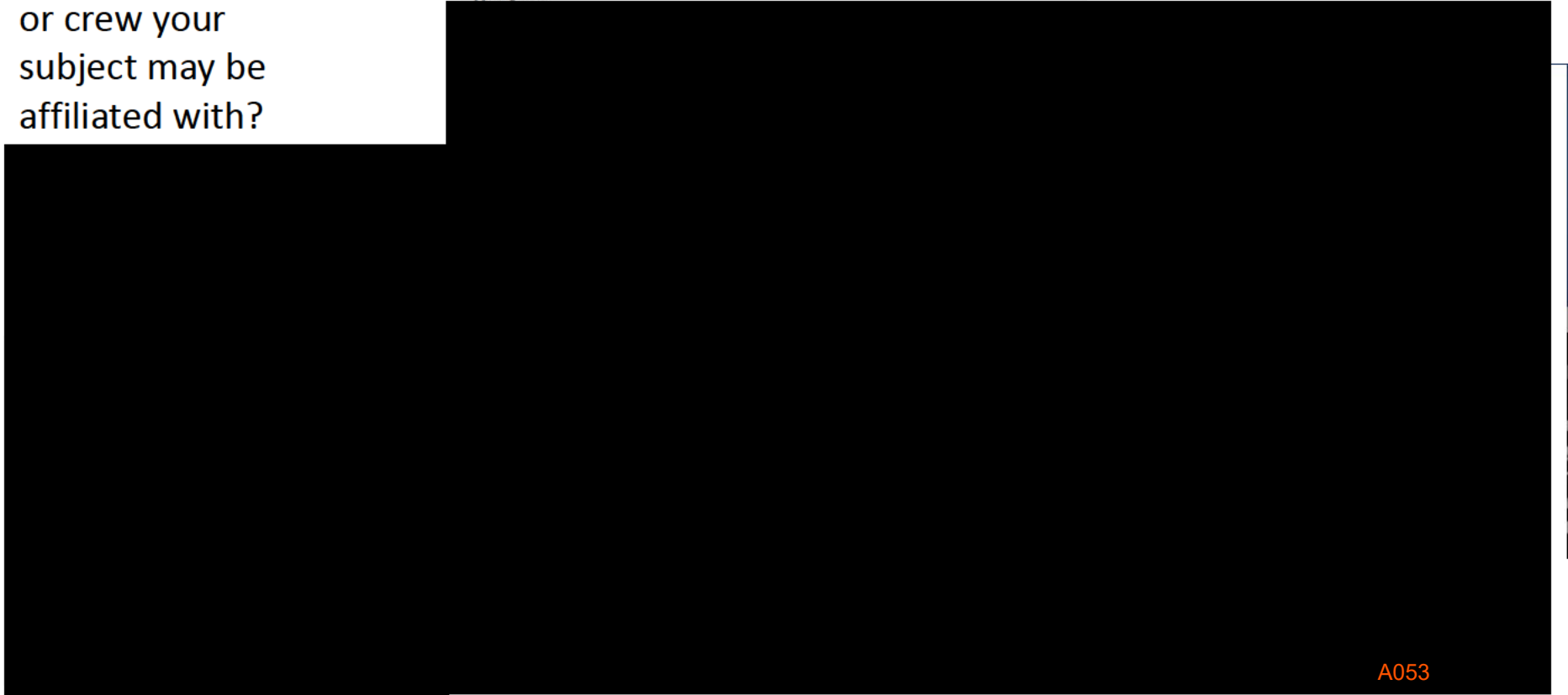


www.instagram.com



INSTAGRAM

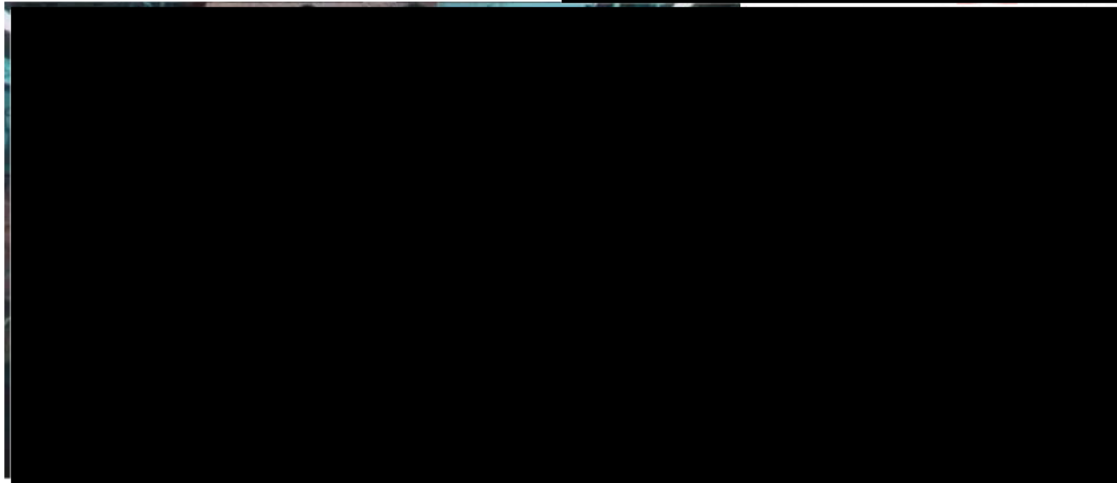
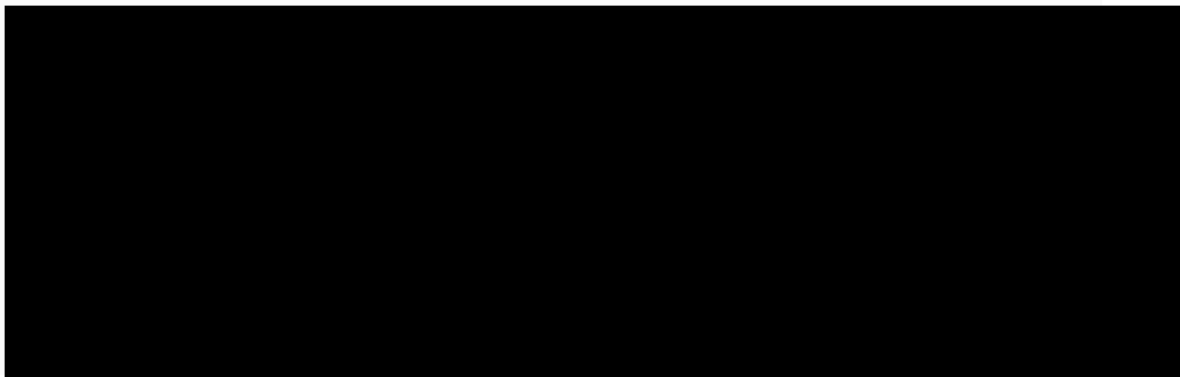
Is there a location
or crew your
subject may be
affiliated with?



A053

INSTAGRAM CONT'D.

While on this profile
look for clues that may
help you identify key
words and help identify
your subject



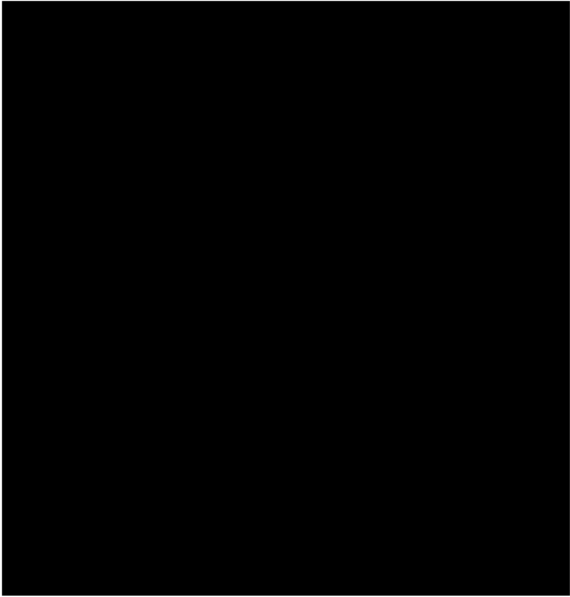
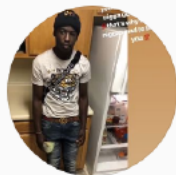
Based on the profile
bio and photos it
appears [redacted] and
[redacted] may be
keywords associated
with subjects from
Simple City

A054

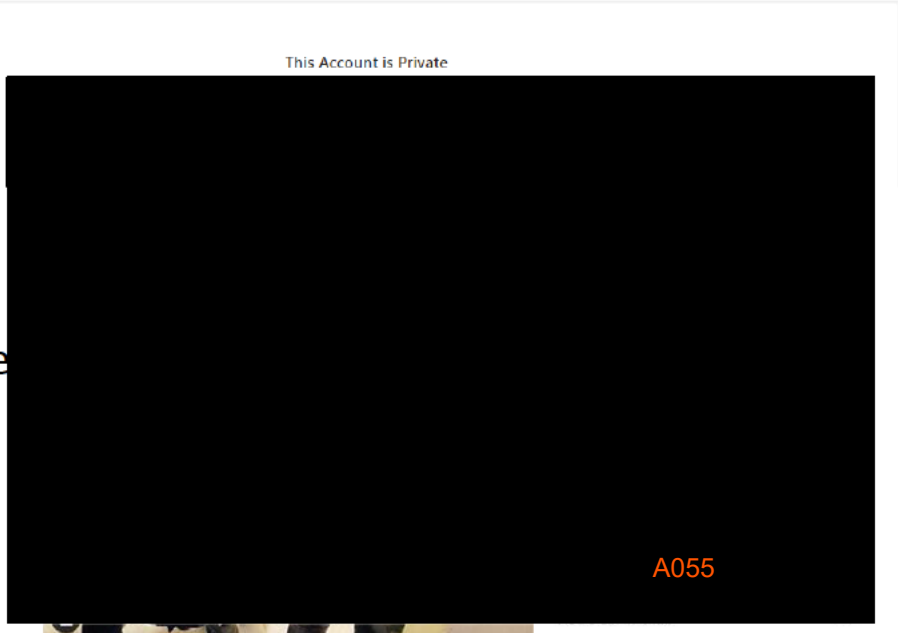
INSTAGRAM CONT'D

Based on that information, try searching [REDACTED] and see what populates

[REDACTED] account is private, how can we combat it?

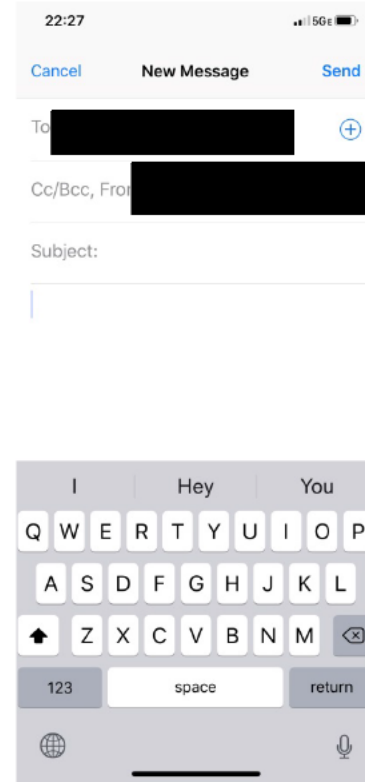
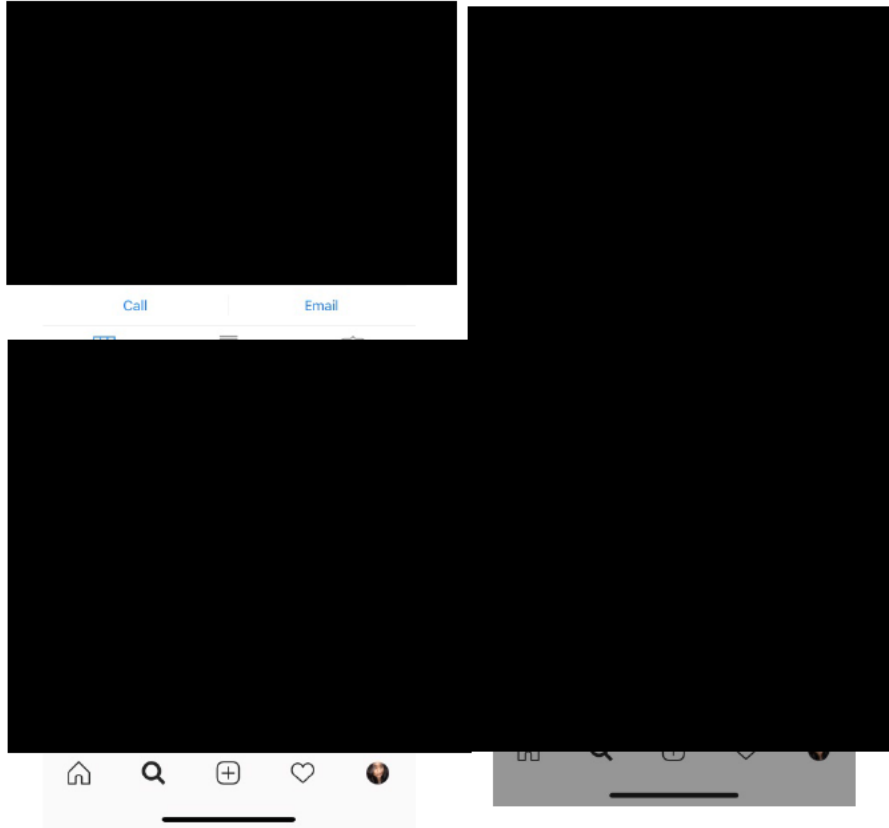


Check [REDACTED] page since its public and he appears to be affiliated with the same area



A055

INSTAGRAM CONT'D



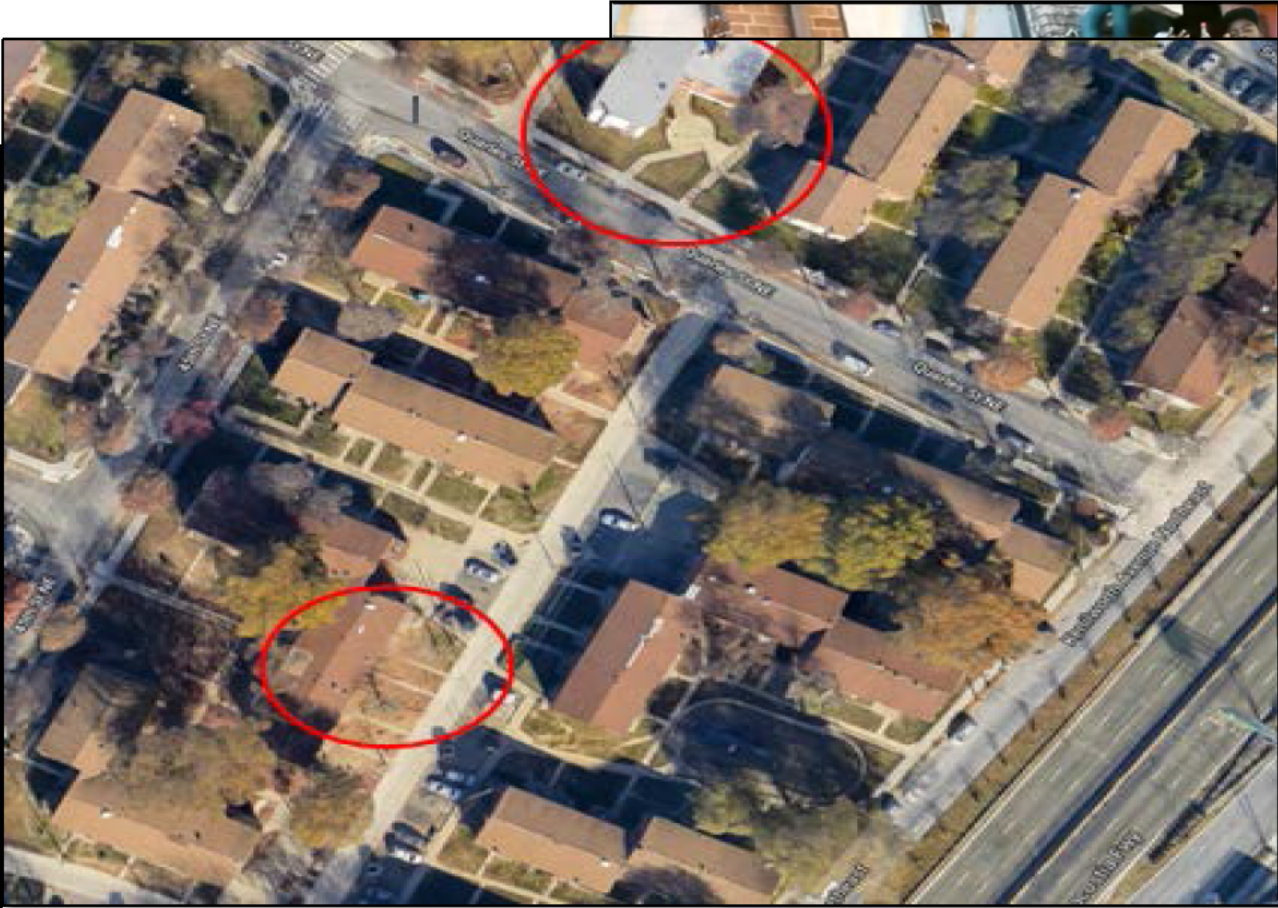
A056

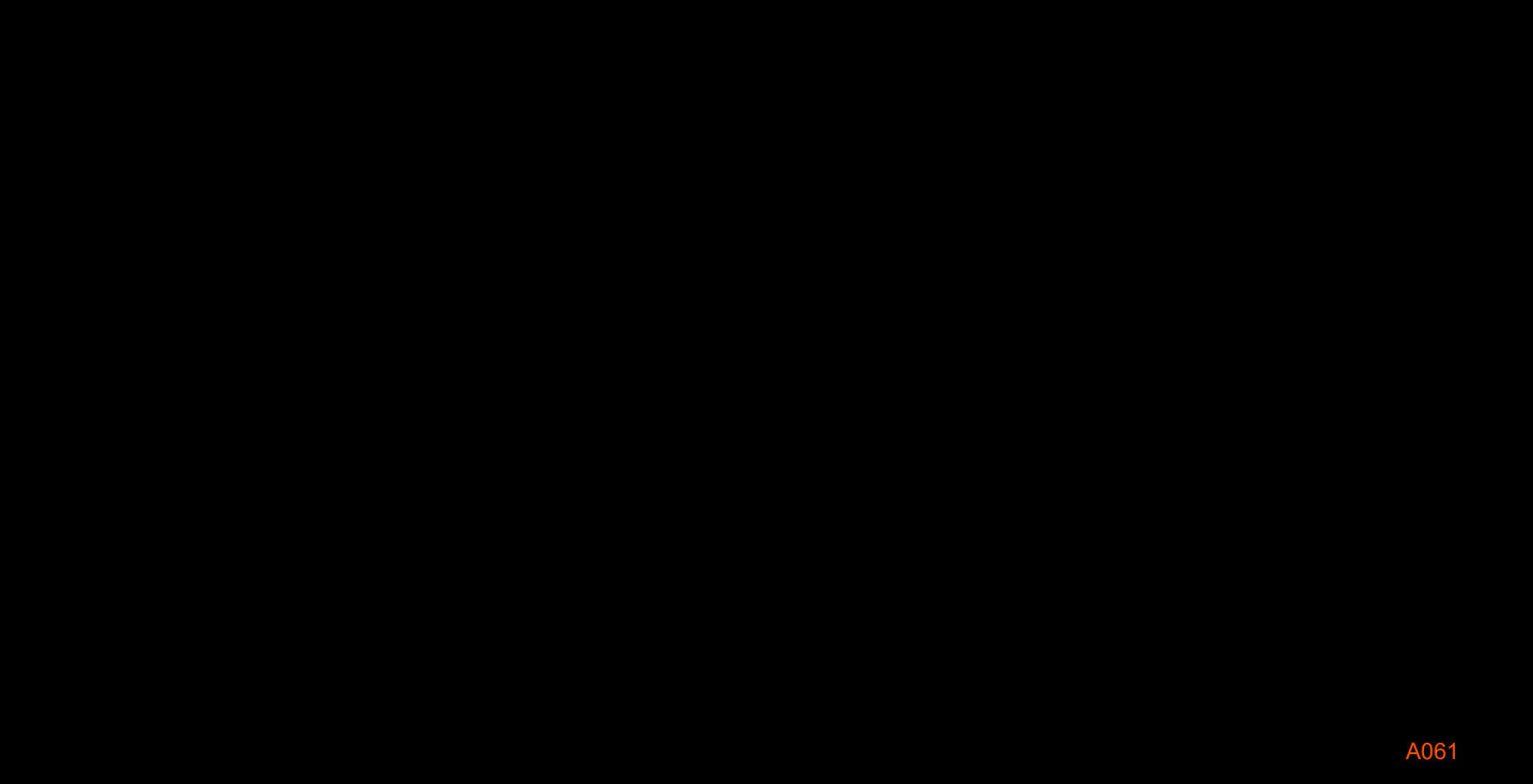
- Social Media drill downs on homicides and high profiles cases/individuals of interest
 - Quick turnaround time for requests
 - Around the clock requests/communication needed between shifts
 - Building out information on hashtags, possible retaliation/crew beefs, relatives/associates
 - Information sharing with Intel, NSID, Districts





SOCIAL MEDIA: TARGETED SEARCHES – YOUTUBE/INSTAGRAM



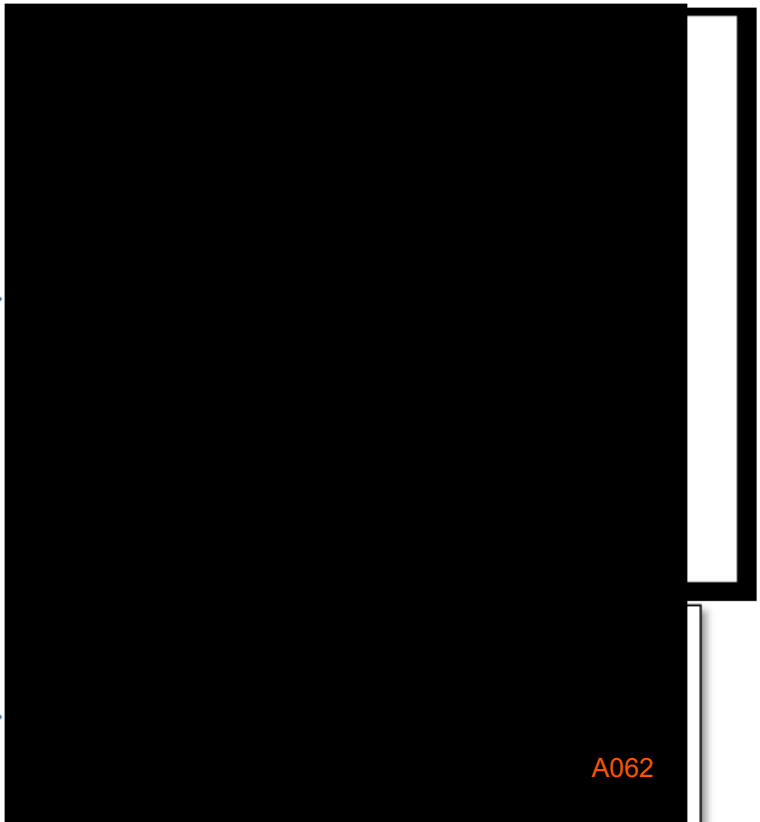
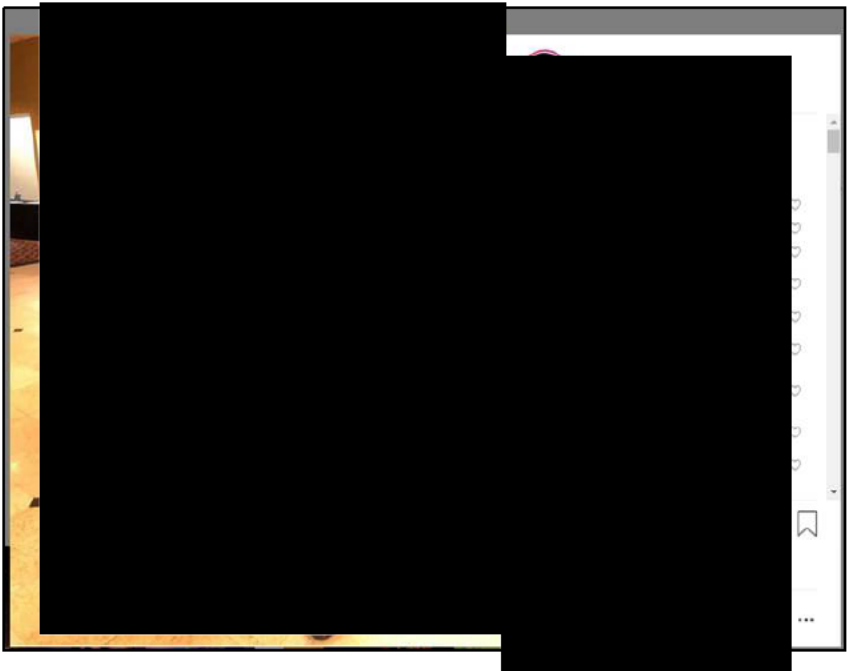


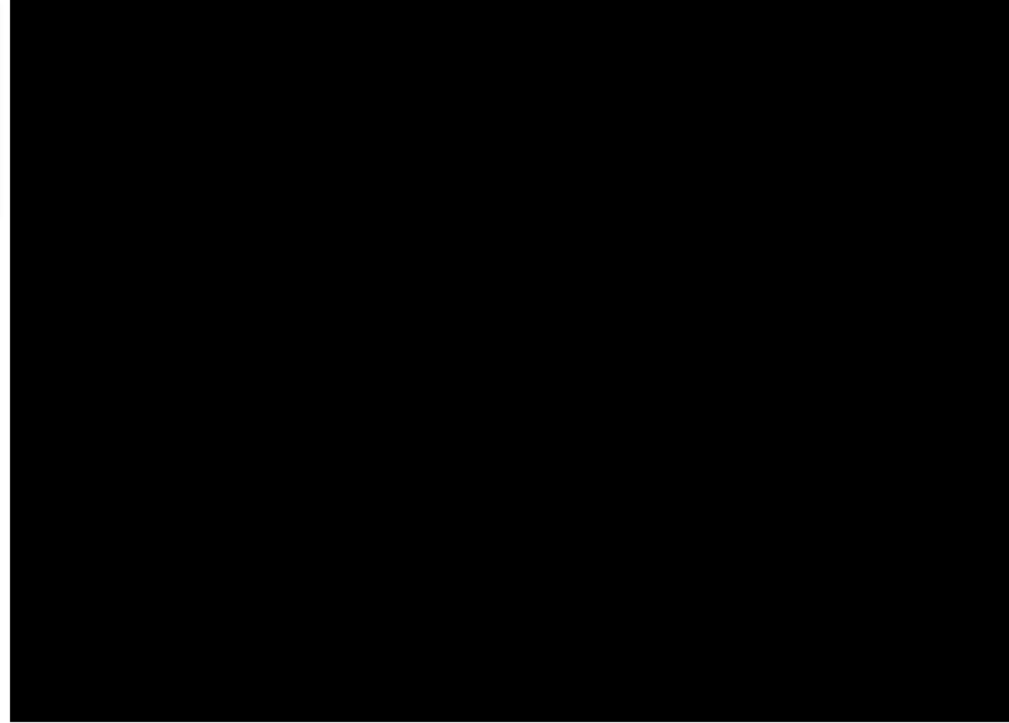
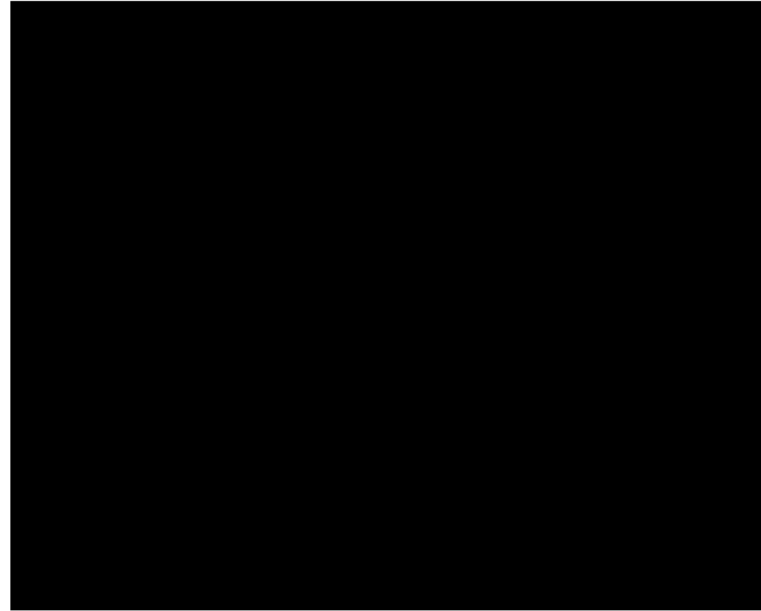
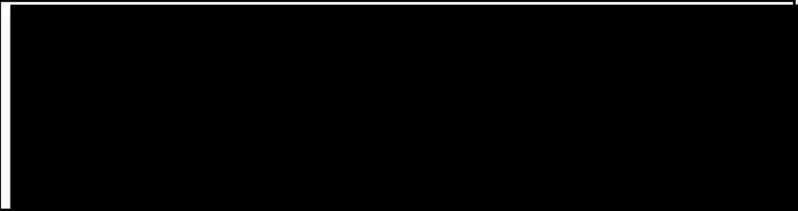


SOCIAL MEDIA: TARGETED SEARCHES - EXAMPLE

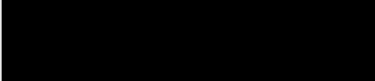
Post homicide follow-up of *validated* [REDACTED]

- Searched through Instagram accounts of known validated members
 - [REDACTED]
 - Posted 4 days after the homicide occurred





Who is this person?



CHALLENGES: SEARCH RESTRICTIONS

The screenshot shows the homepage of 'STORIESDOWN'. At the top, there is a navigation bar with links for 'HOMEPAGE', 'BLOG', 'REMOVE CONTENT', and 'CONTACT US'. The main heading is 'Instagram Story Viewer & Downloader' with a subtitle: 'Best Instagram story viewer! You can watch Instagram stories anonymously and quickly without the need to log in or having account.' Below this is a large white area containing an advertisement for Google with buttons for 'Stop seeing this ad' and 'Why this ad?'. At the bottom of the page, there is a search bar with the placeholder text 'Enter Instagram username' and a 'Search' button. A dark grey navigation bar is partially visible on the left with links for 'Home' and 'Download Stories'.

Start Download
View PDF & Download PDF Converter Guru

Instagram Downloader

INSTADP

Instadp search profile pictures

Search and download Instagram profile pictures or stories

INSTADP STORIES

Q Search username

A065

CHALLENGES: SEARCH RESTRICTIONS INSTADP

INSTADP



Instdp search profile pictures

Search and download Instagram profile pictures or stories

INSTADP STORIES



Search username

INSTADP



Instdp search profile pictures

Search and download Instagram profile pictures or stories

INSTADP STORIES



yln.tay



yln.tay



yln.tayyy



INSTADP

INSTADP

ze and download it

st



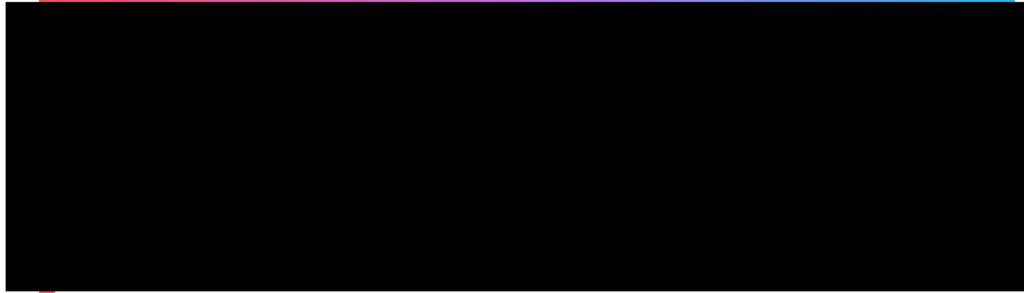
A066

CHALLENGES: SEARCH RESTRICTIONS STORIESDOWN

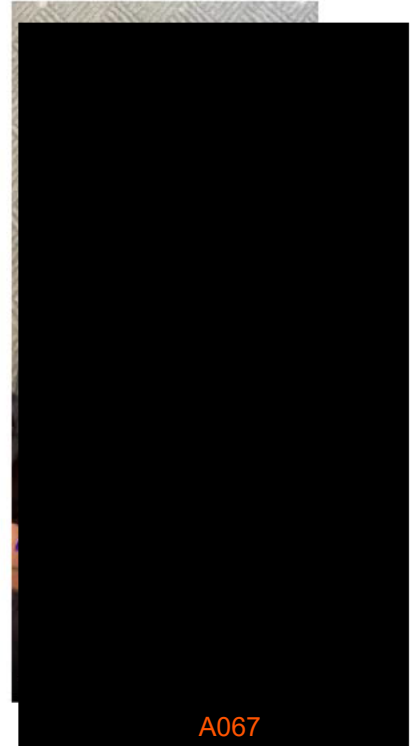


[HOMEPAGE](#) [BLOG](#) [REMOVE CONTENT](#) [CONTACT US](#)

Stories



Posts



A067

5 hours and 42 minutes ago

CHALLENGES: SEARCH RESTRICTIONS W3TOYS



Start Download

View PDF & Download PDF Converter Guru

Inst.

Instagrar

Instagram Downloader

https://www.instagram.com/p/B_Av_YgH1ge/

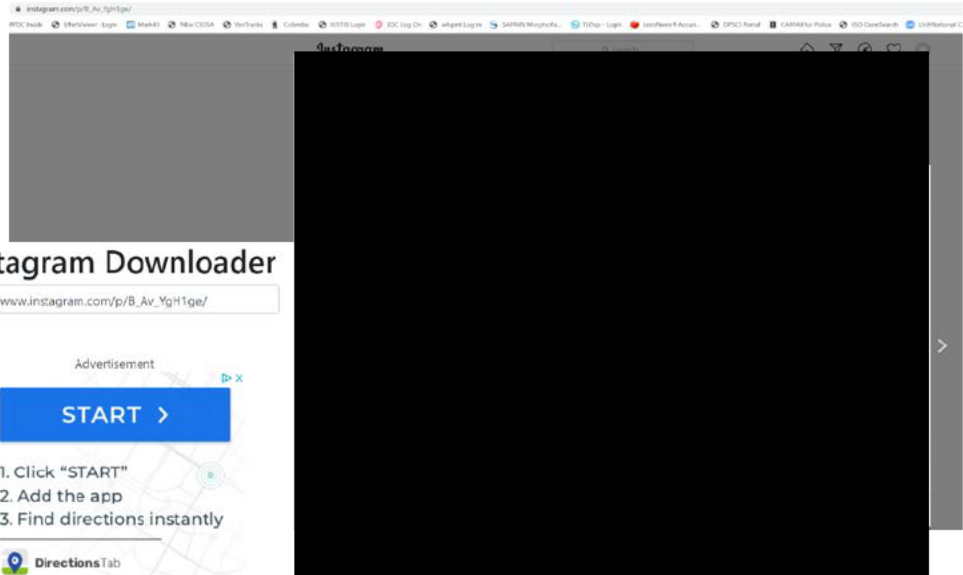
Advertisement

START >

1. Click "START"
2. Add the app
3. Find directions instantly

Directions Tab

Download



CHALLENGES: SEARCH RESTRICTIONS TWITTER DOWNLOAD

Twitter Video Downloader

Download twitter videos & GIF from tweets

←

Ads by Google

Stop seeing this ad Why this ad? ↗

Paste Tweet URL Here:

Enter link/url and click Download

Download

SOCIAL MEDIA: ADDITIONAL SEARCHES



- Using specialized sites to search hashtags, telephone numbers, usernames, email addresses, keywords, URLs
- Specialized site searches for Twitter, Instagram, etc.



peekyou

SPOKEO

pipl

Buzzsumo

Social Searcher

WebMii

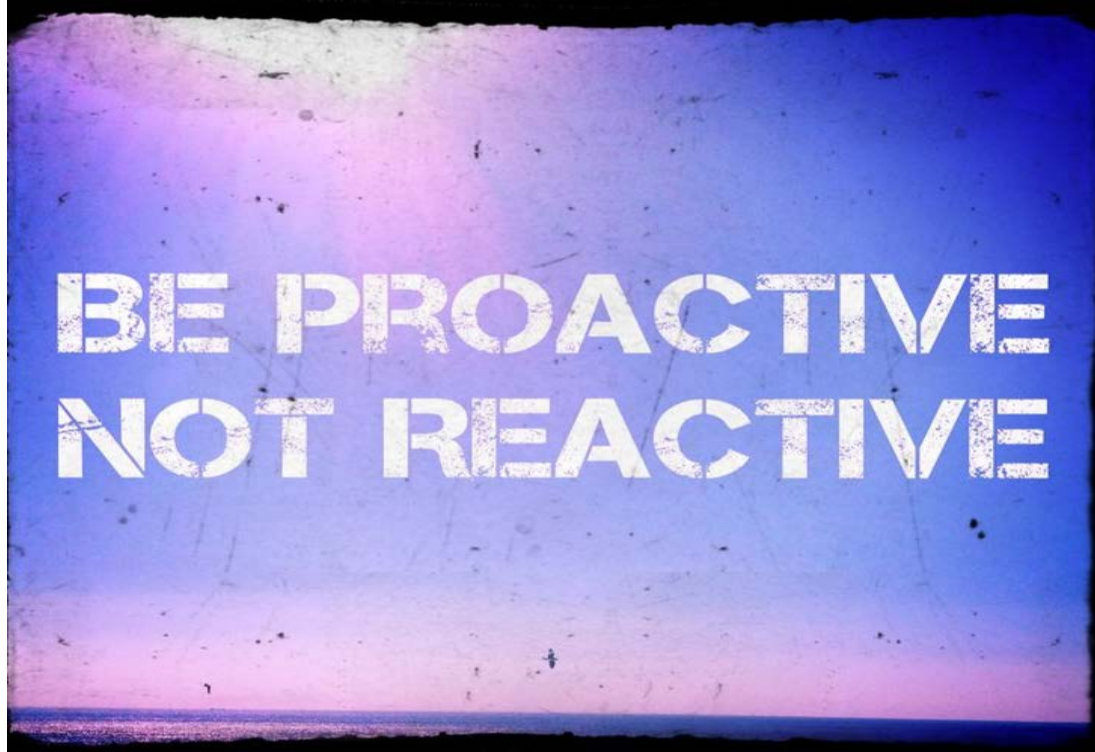
#tagboard

Lullar.com

SnapBird

WEBSTAGRAM

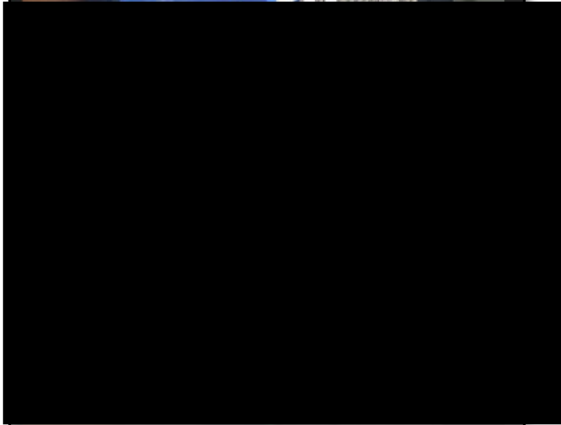
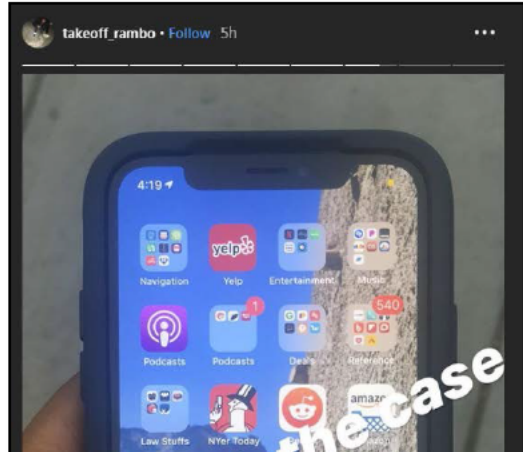
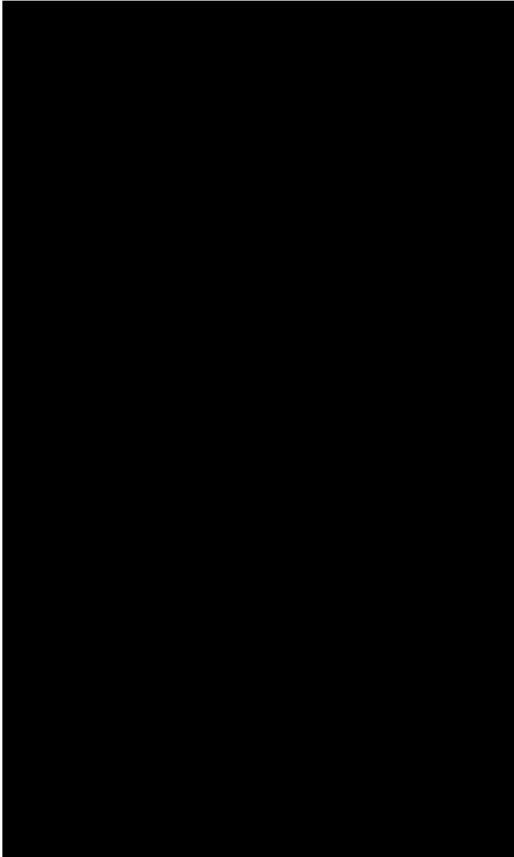
WHAT'S NEXT?



Check-in on known recidivists and gang/crew members with a social media footprint

A071

SOCIAL MEDIA: TARGETED SEARCHES – SUCCESS STORY

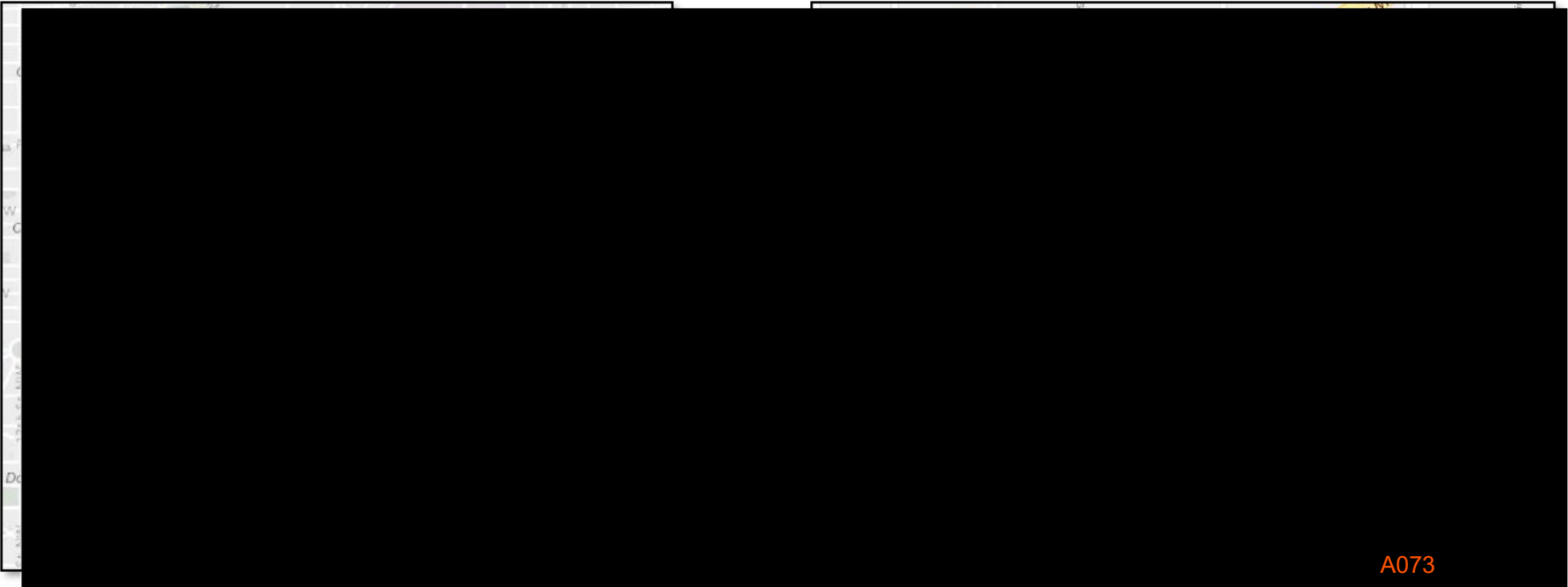


SOCIAL MEDIA: TARGETED SEARCHES - EXAMPLE



01/04/19 0037 - 0234 hours - Robbery (Gun) [REDACTED]

- On the above listed date and time, the complainant and two others were approached from behind and held at gunpoint by three suspects who instructed them to lie face down then took several items including an **iPhoneX** described in Cobalt as **Aluminum/Silver**. The look out in this incident was for **3 B/M, late teens to mid-twenties**.

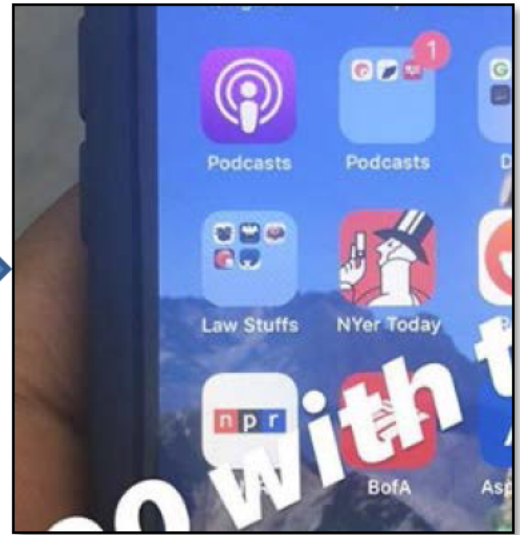
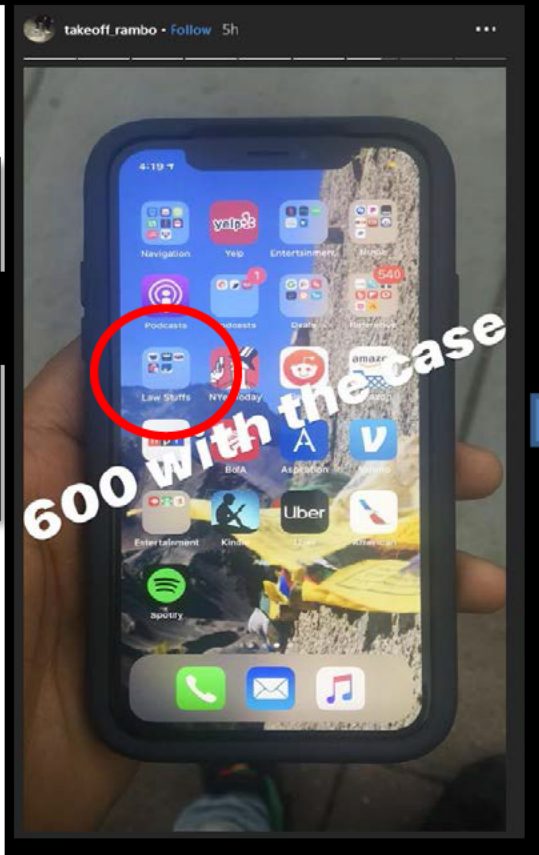




SOCIAL MEDIA: TARGETED SEARCHES - EXAMPLE

Complainant, owner of the iPhone X stolen in the 01/04/19 incident appears to be a lawyer. The phone has a folder of apps dedicate to "Law Stuffs". [REDACTED]

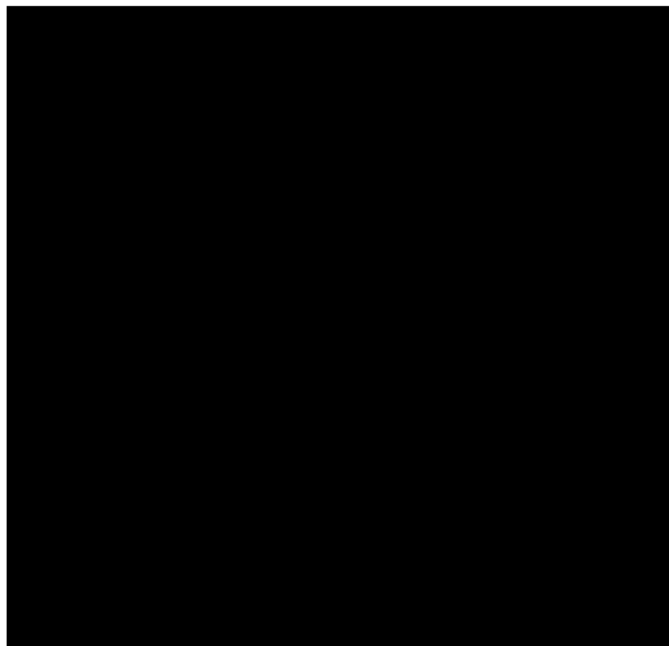
| |
|---|
| Attorney Licensee |
| [REDACTED] |
| License Status: Active |
| [REDACTED] |
| County: Non-California County |
| [REDACTED] |
| Law School: UC Berkeley SOL Boalt Hall; Berkeley CA |



SOCIAL MEDIA: TARGETED SEARCHES - EXAMPLE



Social media was queried for complainant. The following Facebook account was located which matches the complainant based on age and location. Photos show the complainant may have recently visited Asia, possibly China. The background of the phone shown in Logan's Instagram story includes what appear to be Tibetan prayer flags.



- Stopped at the [redacted] probable cause for arrest for being in possession and attempting to sell complainant's phone
- **Placed under arrest for RSP, CPWL, PWID Marijuana**
- Recovered in this incident was a Smith & Wesson 9MM Handgun, 1.8 ounces of marijuana, 2 cell phones

QUESTIONS?



METROPOLITAN POLICE DEPARTMENT

300 INDIANA AVENUE NW – WASHINGTON, DC – 20001 – 202.727.9099

WWW.MPDC.DC.GOV

MEMORANDUM OF UNDERSTANDING

BETWEEN

**DISTRICT OF COLUMBIA HOMELAND SECURITY AND EMERGENCY
MANAGEMENT AGENCY**

AND

DISTRICT OF COLUMBIA METROPOLITAN POLICE DEPARTMENT

I. INTRODUCTION

This Memorandum of Understanding ("MOU") is entered into between the District of Columbia Homeland Security and Emergency Management Agency ("HSEMA"), whose address is 2720 Martin Luther King, Jr. Ave, SE, Washington, DC 20032 and the District of Columbia Metropolitan Police Department ("MPD"), whose address is 300 Indiana Ave, NW, Washington, DC 20001, collectively referred to herein as the "Parties."

II. BACKGROUND

The mission of HSEMA is to ensure that the District of Columbia ("District") is prepared to prevent, protect against, respond to, mitigate and recover from all threats and hazards. As part of this mission, HSEMA oversees the National Capital Region Threat Intelligence Consortium ("NTIC"), which is the District's fusion center. The NTIC employs an all-crimes, all-hazards approach and serves as the National Capital Region's ("NCR") only all-hazards fusion center. The NTIC, which is based in the District of Columbia's Homeland Security and Emergency Management Agency, works in partnership with fusion centers in Maryland and Virginia, as well as the federal government, to conduct regional analysis and share information on terrorism, crime, and natural hazards.

The NTIC is one component of the national network of fusion centers, which the US Department of Homeland Security has sanctioned as a critical strategic initiative for sharing information across a range of natural and manmade threats.

The MPD is the lead public safety agency in the District of Columbia and it is the mission of the MPD to safeguard the District of Columbia and protect its residents and visitors with the highest regard for the sanctity of human life. MPD strives at all times to accomplish the mission with a focus on service, integrity, and fairness by upholding the city's motto *Justitia Omnibus -- Justice for All*.

III. PURPOSE

- A.** The purpose of this MOU is to set forth the terms by which MPD agrees to commit personnel resources and to contribute information to the NTIC. This effort will ensure increased communication and coordination and assist in developing methods to efficiently analyze relevant information at all levels to maximize the usefulness of the NTIC products and increase its usefulness to MPD and other public safety stakeholders in the National Capital Region (NCR).
- B.** This MOU is an agreement among the Parties and is not intended, and should not be construed, to create or confer any other person or entity any right or benefit, substantive or procedural, enforceable at law or otherwise against MPD, NTIC, or any state, locality, or other sponsor under whose auspices a party is participating in the NTIC, or the officers, directors, employees, detailees, agents, representatives, task force members contractors, subcontractors, consultants, advisors, successors, assignees, or other agencies thereof.

IV. RESPONSIBILITIES OF MPD UNDER THIS MOU

- A.** MPD agrees to detail one Liaison Officer ("LNO"), at the rank of Captain or above, to the NTIC. The daily schedule and the hours to be worked by the LNO will be determined by the Parties. This LNO is an addition to the MPD LNO who now supports the Joint All-Hazards Operations Center (JAHOC) within HSEMA, which is the District's 24/7 watch center.
- B.** Responsibilities for the conduct of the MPD LNO, both personally and professionally, shall remain with MPD. During this detail, the LNO will continue to work under the rules and regulations applicable to MPD employees and will be subject to the same personnel rules, regulations, laws and policies, including ethical standards, applicable to those employees. The LNO will report personnel and administrative matters to the commanding official of the Joint Strategic & Tactical Analysis Command Center within MPD.
- C.** The designated MPD LNO will:
 - 1.** Be assigned to work within the Analysis Center of the NTIC.
 - 2.** Oversee the handling and dissemination of all law enforcement information.
 - 3.** Facilitate relevant intelligence to MPD.
 - 4.** Review suspicious activity reports and ensure they are appropriately disseminated within a timely manner to the appropriate agency or unit.
 - 5.** Serve as the MPD representative to HSEMA for information needs associated with special events and emergency activations.

6. Participate in other related matters associated with the HSEMA and NTIC's work with MPD.
7. Be available after normal business hours for responses and liaison needs of the NTIC.
8. Coordinate access to the appropriate law enforcement databases to only the NTIC intelligence analysts who work directly with and are supervised by the MPD LNO.

V. RESPONSIBILITIES OF HSEMA UNDER THIS MOU

- A. As the primary fusion center for the District of Columbia, the NTIC conducts analysis, facilitates information sharing, and assists law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism.
- B. The NTIC shall:
 1. Allow the MPD LNO access to the NTIC at all times.
 2. Provide the MPD LNO with an identification card or credentials.
 3. Provide a standard size work station equipped with a computer and telephone.
 4. Provide appropriate training to the MPD LNO.
 5. Authorize the MPD LNO to oversee NTIC intelligence analysts in any and all work related to law enforcement information activities within the NTIC.
 6. Send any law enforcement related work products (For example: "Daily Officer Awareness Bulletins", "Intelligence Bulletins", "Special Event Threat Assessments", and regional products), prior to publishing, to the MPD LNO for review and approval. The MPD LNO shall have final approval for any analysis, report, or work product developed using MPD data.
 7. Research and disseminate Requests for Information (RFI) and Requests for Analysis (RFA) from law enforcement agencies Monday through Friday during normal business hours, excluding holidays. Any questions regarding a RFI or RFA shall be directed to the MPD LNO.
 8. Leverage NTIC real-time open source research and analysis (ROSA) tools for the MPD Intelligence Branch and grant access to MPD members for outside normal business hours and during holidays.

9. Assist with MPD's Capital Watch and suspicious activity reporting public awareness campaigns
10. Monitor social media, open source websites, news outlets, the HSIN-Sit room, and any additional internal and external resources, in an effort to identify events that could affect the operational landscape or MPD operations, and subsequently provide timely and accurate situational awareness and operational intelligence to MPD personnel.
11. Share Suspicious Activity Reports, Terrorist Screening Center Reports, and all other analysis work products with MPD, especially when utilizing MPD databases and resources.

VI. DURATION OF THIS MOU

The term of this MOU continues in force until terminated. This MOU may be terminated at will by any Party, as long as written notice is provided to the other Party of not less than sixty (60) days. Upon termination of this MOU, all equipment will be returned to the supplying Party.

VII. FUNDING

This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of the understanding between the Parties to commit resources to the NTIC. Unless otherwise agreed in writing, each Party shall bear its own costs in relation to this MOU. Expenditures by each Party will be subject to each organization's budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate additional funds for such expenditures.

VIII. PRIVACY AND CIVIL LIBERTIES

- A. The Parties agree to comply with all applicable law protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information through the NTIC, including, to the extent applicable, the privacy guidelines established for the Information Sharing Environment created by § 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004.
- B. Each Party agrees that the fusion center has now, or will develop, a privacy policy that comports, to the extent practicable, with the Privacy Policy Development Guide published by the Department of Justice as part of the Global Information Sharing Initiative.
- C. This MOU does not alter the Parties' civil and financial liabilities, if any and pursuant to applicable law. MPD shall not be responsible for any civil or financial claim which

does not arise from an act or omission of an employee of MPD committed within the scope of this or her employment.

IX. NOTICE

The Following individuals are the contact points for each Party under this MOU:

Justin Pierce
Deputy Chief and Executive Director
Homeland Security Division
National Capital Region Threat Intelligence Consortium
DC Homeland Security and Emergency Management Agency
2720 Martin Luther King, Jr. Avenue, SE
Washington, DC 20032
(C) 202-437-2348

Carolyn Montagna
Acting Director
Joint Strategic & Tactical Analysis Command Center
Metropolitan Police Department
300 Indiana Ave NW
Washington, DC 20001
(C) 202-489-7859

The Parties may change the contact points at will.

X. MODIFICATIONS

The terms and conditions of this MOU may be modified only upon prior written agreement by the Parties.

XI. MISCELLANEOUS

The Parties shall comply with all applicable laws, rules, and regulations whether now in force or hereafter enacted or promulgated.

IN WITNESS WHEREOF, the parties hereto have executed this MOU as follows:

**DISTRICT OF COLUMBIA HOMELAND SECURITY AND EMERGENCY
MANAGEMENT AGENCY:**



CHRISTOPHER RODRIGUEZ
DIRECTOR, HSEMA

Date: 6/17/19

DISTRICT OF COLUMBIA METROPOLITAN POLICE DEPARTMENT:



PETER NEWSHAM
CHIEF, MPD

Date: JUN 14 2019