

# Ballard Spahr LLP

1909 K Street, NW  
12th Floor  
Washington, DC 20006-1157  
TEL 202.661.2200  
FAX 202.661.2299  
www.ballardspahr.com

Alia L. Smith  
Tel: 202.508.1125  
smithalia@ballardspahr.com

Margaret N. Strouse  
Tel: 202.661.7670  
strousem@ballardspahr.com

December 22, 2021

## VIA EMAIL

The Mayor's Office of Legal Counsel  
FOIA Appeal  
1350 Pennsylvania Avenue, N.W., Suite 407  
Washington, D.C. 20004  
foia.appeals@dc.gov

Re: Freedom of Information Act Appeal  
FOIA Request No. 2021-FOIA-01634

Dear FOIA Appeals Officer:

We write to appeal the partial constructive denial of the above-referenced District of Columbia Freedom of Information Act ("DC-FOIA") request submitted by Data for Black Lives ("D4BL") and the Brennan Center for Justice at NYU School of Law ("Brennan Center") to the Metropolitan Police Department ("MPD"). While MPD did, belatedly, produce some of the documents subject to the request, that production itself makes clear that MPD possesses or has control over many additional documents that it should have produced, but did not.

## **BACKGROUND**

The Brennan Center tracks and reports on, among other things, police departments' social media monitoring – *i.e.*, the collection of information about groups and individuals from social media platforms like Facebook, Twitter, Snapchat, and Instagram. D4BL engages in advocacy to limit police access to technology and data analytics, including through its *#NoMoreDataWeapons* campaign. In furtherance of their mission to understand and explain the police's use of social media monitoring, D4BL and Brennan Center requested, on December 15, 2020, copies of public records related to MPD's training and use of social media monitoring. (A copy of the request is attached as Exhibit A). As more explicitly set forth in Exhibit A, they requested:

1. Policies governing MPD's use of social media monitoring;
2. Records reflecting the MPD's use of social media monitoring;

3. Purchase agreements with or orders from third-party social media monitoring services, including, but not limited to, Dataminr, Geofeedia, Snaptrends, Firestorm, Media Sonar, and others;
4. Records reflecting interactions between police and civilians on social media;
5. Records concerning the use of social media data in criminal investigations;
6. Records concerning the use of social media for other purposes;
7. Records concerning audits or internal reviews of MPD's use of social media monitoring;
8. Training materials regarding the use of social media monitoring;
9. Records reflecting the legal justification(s) for the use of social media monitoring;
10. Records reflecting formal complaints, FOIA requests, or legal challenges regarding MPD's use of social media monitoring;
11. Records reflecting communications with the federal government regarding social media monitoring;
12. Nondisclosure agreements with third-party vendors;
13. Vendor communications, including sales materials, licensing agreements, emails, etc.

Ex. A. The request was assigned handling number 2021-FOIA-01634.

The DC-FOIA required a response by March 24, 2021 under the extended DC-FOIA deadline for requests received during the Initial Covid-19 closure. D.C. Code § 2-532(c)(3)(A) (emergency amendment expired Mar. 22, 2021); *FOIA Tolling Emergency Amendment Act of 2020*, D.C. Act 23-555, effective Dec. 22, 2020 (amending D.C. Code § 2-532(c) through Mar. 22, 2021). On September 30, 2021, more than six months after MPD's statutory response deadline passed, with persistent follow up by D4BL and Brennan Center,<sup>1</sup> and under threat of litigation, MPD finally responded by providing a limited set of documents to Brennan Center and D4BL. By email that same date, MPD also provided correspondence listing certain responsive documents available online, describing information responsive to the request, and indicating it was closing the request. (A copy of this email is attached as Exhibit C.) However, the

---

<sup>1</sup> See Ex. B.

documents MPD produced and pointed to online expressly reference *other*, unproduced, documents that are responsive to D4BL and Brennan Center's request. Therefore, MPD's search for records and production of documents was incomplete.

Accordingly, pursuant to D.C. Code § 2-532(e) and D.C. Code § 2-537(a), D4BL and Brennan Center hereby appeal the constructive partial denial of D4BL and Brennan Center's request to the extent that readily identifiable and responsive documents have been neither produced nor the subject of any specific assertion of an exemption by MPD. The Mayor should direct MPD to (1) conduct an adequate search for the requested records and (2) produce all responsive records, whether or not specifically discussed herein, without further delay.

### **ARGUMENT**

DC-FOIA enacts a broad disclosure policy that requires construing the law "with the view toward expansion of public access and the minimization of costs and time delays to the persons requesting information." *Fraternal Order of Police v. District of Columbia*, 79 A.3d 347, 354 (D.C. 2013) (citing D.C. Code § 2-531). The right of access must be "generously construed." *Id.*; accord *Fraternal Order of Police v. District of Columbia*, 82 A.3d 803, 813 (D.C. 2014).

To comply with its DC-FOIA obligations, the MPD is required to expend all "reasonable efforts" to uncover all relevant documents. *Fraternal Order of Police v. District of Columbia*, 139 A.3d 853, 865 (D.C. 2016). The agency has the burden of establishing *beyond material doubt* that its effort was reasonable. *Id.* MPD must describe, in reasonable detail, where it searched for the requested documents and how its search method was reasonably calculated to uncover all relevant documents. *Doe v. D.C. Metro. Police Dep't*, 948 A.2d 1210, 1220-21 (D.C. 2008). To the extent MPD withholds documents in full or in part, MPD bears the burden of providing the specific exemption and its justification for withholding the documents, so that the Mayor's Office can determine whether MPD has properly invoked the exemption. 1 DCMR 412.5 (providing the agency should provide a "Vaughn index of documents withheld, an affidavit or declaration of a knowledgeable official or employee testifying to the decision to withhold documents, or such other similar proof" for all exempt materials); see *FOP*, 79 A.3d at 358.

Here, as an initial matter, with respect to all the enumerated requests, MPD has failed to describe what systems were searched, what search terms were used, and why it employed such search strategy to locate documents responsive to the request. MPD's email merely describes that "a search" was conducted, Ex. C, making it difficult for D4BL and Brennan Center to assess the reasonableness of MPD's search effort at all, much less determine if MPD has met its burden beyond material doubt. Still, in light of the information that D4BL and Brennan Center do know – from documents produced in response to this request, from documents produced in response to

other DC-FOIA requests, and from their expertise in this area – it is apparent that MPD’s search was inadequate and its production incomplete. For example:

- **Request 1 (Social Media Monitoring Policies):** Among other things, MPD produced “ISS Social Media Procedures,” attached as Exhibit D, in response to Brennan Center and D4BL’s request for social media monitoring policies. *See* Ex. A (Request 1). ISS Social Media Procedures (Ex. D) describes three separate responsive, but unproduced, documents on the first page: “CRS Social Media Passwords,” “ISS Online Resources,” and “Social Media Search Techniques.” Ex. D.

In addition, D4BL and Brennan Center are aware of an additional policy, available in redacted form at [https://cdn.muckrock.com/foia\\_files/2017/01/26/Social\\_media\\_FOIA\\_.pdf](https://cdn.muckrock.com/foia_files/2017/01/26/Social_media_FOIA_.pdf) (attached as Exhibit E), which was not produced or referenced in MPD’s responsive email. MPD is required to produce this form in full to D4BL and Brennan Center or, at a minimum, explain the legal basis for the redactions. *FOP*, 82 A.3d at 813 (an agency bears the burden of demonstrating it properly claimed exemptions for both redactions and withheld documents).

- **Requests 1 and 4 (Policies and Police Interactions with Civilians):** In its request, Brennan Center and D4BL sought, in part, policies related to the use of fictitious or undercover online personas and communications between uniformed or undercover police employees and civilians. Ex. A (Requests 1 and 4). MPD responded that no records relating to fictitious online personas or accounts were located and that Joint Strategic and Tactical Analysis Command Center (“JSTACC”) members “do not create fictitious online personas or interact in an undercover capacity on social media.” Ex. C. However, the produced ISS Social Media Training (attached as Ex. F) suggests that the solution to “Getting Blocked” is to “Change username.” *See* Ex. F at 6. It strains credulity to suggest that changing usernames would be an effective solution to getting blocked if the MPD officer’s second username was not an undercover or alias account. In light of these policies, it is clear that additional documents must exist.
- **Request 2 (Use of Social Media Monitoring):** Brennan Center and D4BL requested, in part, “[a]ny and all recordkeeping, logs, or digests reflecting the use of social media monitoring.” *See* Ex. A (Request 2). In its email, MPD is silent on the existence of recordkeeping or digests; instead it provided only the narrow response that “[a] search located no records of *logs* reflecting social media searches.” *See* Ex. C (emphasis added). However, the publicly-available 2013 Social Media Monitoring Policy (Ex. E) states that officers shall “print or

document information” gathered via social media, submit an oral or written request before interacting on social media in exigent circumstances, provide a written request for a social media monitoring extension to continue for longer than thirty days, and “prepare a weekly report.” Under this policy, Lieutenants also “shall maintain a file of all requests.” *Id.* Further, MPD’s ISS Social Media Procedures (Ex. D) includes *templates* to document social media searches within a crime report’s “social media section.” MPD therefore must have records of social media monitoring searches because its policies require record-keeping and even provide templates for such purposes.

- **Request 3 (Social Media Monitoring Purchase Agreements and Orders):** In response to D4BL and Brennan Center’s request for purchase agreements and orders of social media monitoring services, MPD asserts that the only social media monitoring application it can access is Dataminr, which was purchased by three other agencies: the Office of the Chief Technology Officer (“OCTO”), Homeland Security Emergency Management Agency (“HSEMA”), and National Technology Information Center (“NTIC”). *See* Ex. C. However, the Office of Contracting and Procurement (“OCP”) released public records revealing several purchases of Babel Street, another social media monitoring application, by HSEMA, in response to a separate DC-FOIA request by Brennan Center and D4BL.<sup>2</sup> OCP provided order forms, invoices, and statements of work for several Babel Street subscription purchases by HSEMA. If MPD has access to Dataminr through HSEMA’s subscription, it follows that MPD is likely to have access to all of HSEMA’s social media monitoring tools, like Babel Street. MPD must search for and produce all records that document its access and use of Babel Street.

In addition, MPD’s email states that MPD did not locate any records of contracts for social media monitoring applications, and that its *only* access to Dataminr is through a purchase by OCTO, HSEMA, and NTIC. *See* Ex. C. This directly contradicts a donation report published by the Office of Partnerships and Grant Services (“1st Quarter Report on Donations Approved by the DC Office of Partnerships and Grant Services”), an online public record that was *specifically referenced* in the DC-FOIA request. *See* Ex. A at n.6. This document indicates that Dataminr donated training services for 10 officers, valued at \$10,000, in

---

<sup>2</sup> Sent by Brennan Center and D4BL on February 17, 2021 and assigned FOIA Request No. 2021-FOIA-03164.

December of 2016.<sup>3</sup> MPD failed to disclose any purchase agreements, orders, contracts, or vendor communications (including attachments to communications), related to Dataminr's 2016 donation.

- **Requests 3, 4, 12 & 13:** The document produced by MPD titled "ISS Social Media Training Updated" references multiple social media monitoring services MPD uses, such as storiesig.com, Spokeo, Pipl, Webstagram, Facebook Messenger, LexisNexis Accurint, TransUnion TLOxp, Buzzsumo, WebMii, Tagboard, Lullar, SnapBird, and Social Searcher. *See* Ex. F at 6, 8, 28. Despite seemingly providing these services to their officers, MPD indicated that it "does not have any contracts with any social media vendors" and failed to produce *any* purchase agreements and orders, vendor communications, social media account information from civilians, nondisclosure agreements, or other documents providing usage of these services as requested by D4BL and the Brennan Center by Requests 3, 4, 12, and 13. *See* Ex. A.
- **Request 8 (Training Materials):** In response to Brennan Center and D4BL's request for training materials that discuss social media monitoring, Ex. A (Request 8), MPD produced two undated training presentations: (1) 081920 Investigator Training - Emergency Disclosures and (2) ISS Social Media Training Updated. ISS Social Media Training Updated references "old procedures," none of which have been produced. *See* Ex. F at 4-5.

In sum, there are abundant indications that MPD did not conduct a thorough search and did not produce all documents responsive to D4BL's and Brennan Center's DC-FOIA request. Accordingly, D4BL and Brennan Center seek as relief in connection with this administrative appeal an instruction that MPD conduct a complete and thorough new search and provide a statement explaining its search methods (including search terms, databases searched, and search strategy). In addition, D4BL and Brennan Center seek immediate production of the following documents, which should have been included in MPD's initial response:

- Any and all records that document MPD's access to and use of Babel Street, including but not limited to communications with or about Babel Street (including all attachments to those communications), memorandums of use, contracts, training materials, purchase agreements, and orders.

---

<sup>3</sup> *See*

[https://opgs.dc.gov/sites/default/files/dc/sites/opgs/page\\_content/attachments/1st%20Quarter%20FY17%20Donations%20Report\\_0.pdf](https://opgs.dc.gov/sites/default/files/dc/sites/opgs/page_content/attachments/1st%20Quarter%20FY17%20Donations%20Report_0.pdf) at 5.

- Any and all records related to Dataminr's 2016 donation to MPD, including but not limited to any purchase agreements, orders, contracts, training materials, memorandums of use, or communications with or about Dataminr (including all attachments to those communications).
- The following documents referenced in ISS Social Media Procedures (Ex. D) and all other documents contained in the referenced "Social Media folder": "CRS Social Media Passwords," "ISS Online Resources," and "Social Media Search Techniques."
- Records reflecting the dates that the following training presentations, produced in response to Request 8, were created and used: (1) 081920 Investigator Training - Emergency Disclosures and (2) ISS Social Media Training Updated (Ex. F).
- MPD's "old procedures", including any drafts of past or current policies or procedures, referenced in ISS Social Media Training Updated. Ex. F at 4-5.
- Purchase agreements and orders, vendor communications (including all emails, attachments, sales materials, licensing agreements, memorandums), social media account information from civilians, nondisclosure agreements, memorandums of understanding, or other documents related to MPD's use of storiesig.com, Spokeo, Pipl, Webstagram, Facebook Messenger, LexisNexis Accurint, TransUnion TLOxp, Buzzsumo, WebMii, Tagboard, Lullar, SnapBird, and Social Searcher. *See* Ex. F at 6, 8, 28.
- Any and all recordkeeping related to social media monitoring searches, including but not limited to all written requests for monitoring extensions, weekly reports, and files of requests pursuant to the 2013 social media monitoring policy, Ex. E, and all crime report social media sections, as referenced in ISS Social Media Procedures (Ex. D) template.<sup>4</sup>

---

<sup>4</sup> In addition, D4BL and Brennan Center seek clarification regarding MPD's response to Request No. 5, regarding the use of social media in criminal investigations. MPD stated that it "has no records responsive to this portion of the request." Ex. C. However, it did produce a document entitled "Crime 01.01.13 Through 12.12.2020," attached as Exhibit G, reflecting general crime statistics for the time period. D4BL and Brennan Center request explanation of whether this document contains crimes in which social media monitoring was used and whether it is responsive to Request 5.

- Policies, protocols, and other documents related to usernames officers have available to “change” to when blocked, Ex. F at 6, and the use of fictitious or anonymous online personas used by MPD.

\* \* \*

We look forward to your prompt response within 10 business days of this appeal. *See* D.C. Code § 2-537(a). Should you like to discuss the request or this appeal, please do not hesitate to contact us. Thank you.

Sincerely,

BALLARD SPAHR LLP

A handwritten signature in blue ink that reads "Alia Smith". The signature is fluid and cursive, with a long horizontal stroke at the end.

Alia L. Smith  
Margaret N. Strouse

Encls.

cc: Brennan Center  
D4BL  
Robert Eckert, MPD FOIA Specialist (Robert.eckert@dc.gov)



# Exhibit A

# BRENNAN CENTER FOR JUSTICE

December 15, 2020

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

Inspector Vendette Parker  
Metropolitan Police Department  
300 Indiana Avenue, NW  
Room 4153  
Washington, D.C. 20001

Via: DC Government Public FOIA Portal

## **Re: Freedom of Information Act Request**

Dear Sir or Madam:

This is a request under the District of Columbia's Freedom of Information Act ("FOIA"), D.C. Code §§ 2-531-539, on behalf of Data for Black Lives and the Brennan Center for Justice at NYU School of Law ("Brennan Center"). Data for Black Lives and the Brennan Center seek information relating to the Metropolitan Police Department's ("MPD's") use of social media to collect information about individuals, groups, and activities, described below as "social media monitoring."

### **Background**

In general, "social media monitoring" is a term describing the use of social media platforms like Facebook, Twitter, Snapchat, and Instagram to gather information for purposes including, but not limited to, identifying potential threats, reviewing breaking news, collecting individuals' information, conducting criminal investigations and intelligence, and gauging public sentiment.

Social media monitoring includes four types of activities: (1) monitoring or tracking an individual, a group, or an affiliation (e.g., an online hashtag) via publicly available information; (2) using an informant, a friend of the target, or an undercover account to obtain information from a protected, private, or otherwise unavailable account or page; (3)

using software like Dataminr to monitor individuals, groups, associations, or locations; or (4) issuing a subpoena, warrant, or other form of legal process to a social media platform for data held by that platform.

Social media is a crucial forum for the exchange of ideas, particularly in this time of unprecedented public activism and political engagement. Social media platforms like Facebook, Twitter, and Instagram have proven to be an invaluable tool for connecting and organizing around a variety of issues and across diverse movements. In a time when social media is recognized as akin to the “modern public square,”<sup>1</sup> social media monitoring has significant civil rights implications. Like other forms of surveillance, social media monitoring impacts what people say and who they interact with online. The deleterious effects of surveillance on free speech have been well documented in empirical research.<sup>2</sup>

Publicly available records indicate the Metropolitan Police Department engages in social media monitoring, including in its criminal investigations and to monitor public events. For example, the Department’s Special Order 13-04, entitled “Investigative Support Unit,” contains an incident response checklist that lists as a potential action: “Establish ‘fence’ for Twitter or conduct other research or investigative actions via social media sites.”<sup>3</sup> Similarly, General Order 803.06 states that, during a major event or critical incident, the Command Information Center Watch Commander shall ensure that “Media outlets and social media are monitored, in coordination with the Intelligence Infusion Division and Public Information Branch, in order to correct mistaken or inaccurate information that is reported and, if corroborated, use the information to assist MPD during the incident in accordance with Departmental policy.”<sup>4</sup> A 2013 memorandum from the Criminal Intelligence Branch described the creation of Social Media Teams to monitor social media

---

<sup>1</sup> *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017) (quoting *Reno v. American Civil Liberties Union*, 521 U. S. 844, 868 (1997)).

<sup>2</sup> See, e.g., Faiza Patel et al., *Social Media Monitoring*, Brennan Center for Justice, May 22, 2019, <https://www.brennancenter.org/publication/social-media-monitoring>; Jonathon W. Penney, “Chilling Effects: Online Surveillance and Wikipedia Use,” *Berkeley Technology Law Journal* 31, no. 1: 117-182 (2016), [https://btlj.org/data/articles2016/vol31/31\\_1/0117\\_0182\\_Penney\\_ChillingEffects\\_WEB.pdf](https://btlj.org/data/articles2016/vol31/31_1/0117_0182_Penney_ChillingEffects_WEB.pdf); Elizabeth Stoycheff, “Under Surveillance: Examining Facebook’s Spiral of Silence Effects in the Wake of NSA Internet Monitoring,” *Journalism and Mass Communication Quarterly* 93, no. 2: 296-311 (2016), <https://journals.sagepub.com/doi/pdf/10.1177/1077699016630255#articleCitationDownloadContainer>; Matthew A. Wasserman, “First Amendment Limitations on Police Surveillance: The Case of the Muslim Surveillance Program,” *New York University Law Review* 90, no. 5: 1786-1826 (2015), <https://www.nyulawreview.org/wp-content/uploads/2018/08/NYULawReview-90-5-Wasserman.pdf>.

<sup>3</sup> Investigative Support Unit, “Criminal Research Specialist Incident Response Checklist,” No. SO-13-04, Metropolitan Police Department, May 14, 2013, [https://go.mpdonline.com/GO/SO\\_13\\_04.pdf](https://go.mpdonline.com/GO/SO_13_04.pdf).

<sup>4</sup> Metropolitan Police Department, “Command Information Center,” No. GO-803.06, May 19, 2015, [https://cdn.muckrock.com/foia\\_files/2017/01/26/GO803.06.pdf](https://cdn.muckrock.com/foia_files/2017/01/26/GO803.06.pdf).

websites for information on criminal activity.<sup>5</sup> The DC Office of Partnerships and Grant Services also revealed that, in December 2016, the Department had received a donation of training services for 10 officers on alerts by Dataminr, a social media monitoring provider.<sup>6</sup>

Despite widespread public interest in social media monitoring by law enforcement officers, the public lacks information about the current capabilities and limitations of the Metropolitan Police Department's social media monitoring operations. We therefore request the documents below.

### **Request**

The Brennan Center specifically requests records under FOIA that were in the Metropolitan Police Department's possession or control from January 1, 2013 through the date of the production of records, in the following categories:

1. **Policies Governing Use:** Any and all department-wide or unit-specific policies, procedures, regulations, protocols, manuals, or guidelines related to:
  - a. the use of social media monitoring by police department employees including, but not limited to, for the purposes of conducting a criminal investigation, undertaking situational awareness activities, monitoring current or anticipated gatherings, or otherwise viewing or gathering information about individuals;
  - b. the authorization, creation, use, and maintenance of fictitious/undercover online personas;
  - c. the collection and maintenance of location data from social media platforms and/or applications; or
  - d. the retention, analysis, or sharing of data collected via social media.
2. **Recordkeeping:** Any and all recordkeeping, logs, or digests reflecting the use of social media monitoring, or searches of social media for purposes including criminal investigations, situational awareness, event planning, or public safety.
3. **Purchase Agreements and Orders:** Any and all records reflecting a contract or agreement to purchase, acquire, use, test, license, or evaluate any product or service

---

<sup>5</sup> Metropolitan Police Department, "Memorandum from Lieutenant Michael J. Pavlik to the Metropolitan Police Department's Criminal Intelligence Branch re: Social Media Monitoring Policy," June 5, 2013, [https://cdn.muckrock.com/foia\\_files/2017/01/26/Social\\_media\\_FOIA\\_.pdf](https://cdn.muckrock.com/foia_files/2017/01/26/Social_media_FOIA_.pdf).

<sup>6</sup> Government of the District of Columbia Office of Partnerships and Grant Services, "1st Quarter Report on Donations Approved by OPGS FY 2017," [https://opgs.dc.gov/sites/default/files/dc/sites/opgs/page\\_content/attachments/1st%20Quarter%20FY17%20Donations%20Report\\_0.pdf](https://opgs.dc.gov/sites/default/files/dc/sites/opgs/page_content/attachments/1st%20Quarter%20FY17%20Donations%20Report_0.pdf).

developed by any company providing third-party social media monitoring services, including, but not limited to, Dataminr, Geofeedia, Snaptrends, Firestorm, Media Sonar, Social Sentinel, or Dunami.

4. **Social Media Account Information from Civilians:** Any and all records reflecting:
  - a. interactions with civilians in which police department employees requested information about the civilian's social media account information, including, but not limited to, a username, identifier, handle, linked email, or password; or
  - b. communications conducted on social media platforms between uniformed or undercover police department employees and civilians, including, but not limited to, direct messages, group messages, chat histories, comments, or "likes."

But excluding communications conducted as part of ongoing investigations and communications appearing on a page or account operated by the MPD and bearing the MPD's name, insignia, or other indicia of ownership or control.

5. **Use for Criminal Investigations:** Any and all records reflecting the number of criminal investigations in which social media research has been used, the number of criminal investigations in which fictitious/undercover online personas have been used, the nature of the offenses charged in those investigations, and the number of those investigations that resulted in arrests and/or prosecutions.
6. **Use for Purposes Other Than Criminal Investigations:** Any and all records reflecting the number of circumstances in which social media was used to collect information about individuals for purposes other than criminal investigations or background checks for police department employment, including regarding protest activity, as well as the number of such matters in which an individual or group was charged with a crime.
7. **Audits:** Any and all records of, or communications regarding, audits or internal reviews of the Department's use of social media monitoring for the purpose of investigations, situational awareness, event planning, intelligence, or public safety, including, but not limited to, records reflecting any disciplinary actions, warnings, or proceedings in response to an employee's use of social media.
8. **Training Materials:** Any and all training documents, including drafts, discussing social media monitoring, including, but not limited to, PowerPoint presentations, handouts, manuals, or lectures.

9. **Legal Justifications:** Any and all records reflecting the legal justification(s) for social media monitoring, including, but not limited to, memos, emails, and policies and procedures.
10. **Formal Complaints, Freedom of Information Requests, and Legal Challenges:** Any and all records reflecting formal complaints, FOIA requests, or legal challenges regarding the Department's use of social media monitoring, including, but not limited to, those complaints or legal challenges made by civilians, non-profit groups, or companies.
11. **Federal Communications:** Any and all records reflecting any communications, contracts, licenses, waivers, grants, or agreements with any federal agency concerning the use, testing, information sharing, or evaluation of social media monitoring products or services. This includes, but is not limited to, records reflecting communications regarding information sharing between MPD and federal law enforcement agencies, such as the FBI, Secret Service, Park Police, ATF, DEA, Bureau of Prisons, U.S. Marshals Service, Capitol Police, Department of Homeland Security's CBP and Border Patrol units, in response to protests in June 2020.<sup>7</sup>
12. **Nondisclosure Agreements:** Any and all records regarding the MPD's nondisclosure or confidentiality obligations in relation to contracts or use agreements with third-party vendors of social media monitoring products or services.
13. **Vendor Communication:** Any and all records reflecting interactions with any third-party vendors concerning social media monitoring products or services, including, but not limited to, sales materials, licensing agreements, communications, memorandums, and emails relating to those products.

### **Fee Waiver and Expedited Processing**

The above requests are a matter of public interest. The disclosure of the information sought is not for commercial purposes; instead, it will contribute to the public's understanding of government operations. Accordingly, Data for Black Lives and the Brennan Center for Justice request a fee waiver and expedited processing pursuant to DC Code § 2-532(b).

---

<sup>7</sup> Office of Public Affairs, "Attorney General William P. Barr's Statement on Protests in Washington, D.C.," Department of Justice, June 2, 2020, <https://www.justice.gov/opa/pr/attorney-general-william-p-barrs-statement-protests-washington-dc>.

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, it is working to support a network of grassroots racial justice organizations to challenge discriminatory uses of data and algorithms across systems. With a national network of thousands of scientists and activists, it is working to build a future in which data and technology are forces for good, rather than instruments of oppression, in Black communities.

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.

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 Data for Black Lives 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 [hecht-felellal@brennan.law.nyu.edu](mailto:hecht-felellal@brennan.law.nyu.edu).

### **Response Required**

The Brennan Center appreciates the Metropolitan Police Department's attention to this request and expects that the Department will send its legally mandated response within fifteen business days of receipt, subject to the possibility of a ten business day extension, as required under DC Code § 2-532. To the extent that the Department withholds any records, please list, in writing, each document that is withheld as well as the specific claimed exemption.<sup>8</sup> We also request that you provide us with the documents in electronic format where possible. If documents must be produced in hard copy, please first contact Laura Hecht-Felella, contact information below.

---

<sup>8</sup> See Washington, DC Municipal Code § 2-533.

Should you have any questions concerning this request, please contact Laura Hecht-Felella by telephone at (646) 292-8385 or via e-mail at [hecht-felella@brennan.law.nyu.edu](mailto:hecht-felella@brennan.law.nyu.edu).

Thank you for your time.

*Laura Hecht-Felella*

Laura Hecht-Felella  
George A. Katz Fellow, Liberty and National Security Program  
Brennan Center for Justice at NYU School of Law  
(646) 292-8385 | [hecht-felella@brennan.law.nyu.edu](mailto:hecht-felella@brennan.law.nyu.edu)



# Exhibit B

**From:** [Eckert, Robert \(MPD\)](#)  
**To:** [Laura Hecht-Felella](#)  
**Cc:** [Sahil Singhvi](#); [Rachel Levinson-Waldman](#); [Archie-Mills, Lisa \(MPD\)](#)  
**Subject:** FOIA Request No. 2021-FOIA-01634, from Ms. Hecht-Fella (Brennan Center)  
**Date:** Wednesday, March 24, 2021 3:54:32 PM

---

Hello Ms. Hecht-Felella,

Thanks for your query.

As you know, the referenced FOIA request consists of a broad variety of thirteen (13) itemized/individual requests for records/information, including those that may not currently exist.

While the District of Columbia (DC) Freedom of Information Act (FOIA) does not require agencies to create records, we are working to address each of the thirteen (13) items/requests, in turn, posed within this FOIA request.

We will respond to the FOIA request upon the completion of the following: the search for records that may be responsive to the request; the review for material that may be exempt from release under the FOIA; and, the completion of any other needed consultation and coordination.

Thanks,  
Bob Eckert  
FOIA Specialist  
MPD FOIA Office  
robert.eckert@dc.gov  
"We are here to help."

---

**From:** Laura Hecht-Felella <hecht-felella@brennan.law.nyu.edu>  
**Sent:** Wednesday, March 24, 2021 1:54 PM  
**To:** Eckert, Robert (MPD) <robert.eckert@dc.gov>; Crumlin, Latrina (MPD) <Latrina.Crumlin2@dc.gov>; Archie-Mills, Lisa (MPD) <lisa.archie-mills@dc.gov>  
**Cc:** Sahil Singhvi <singhvis@brennan.law.nyu.edu>; Rachel Levinson-Waldman <levinsonr@brennan.law.nyu.edu>  
**Subject:** RE: Acknowledgement Letter 2021-FOIA-01634

**CAUTION:** This email originated from outside of the DC Government. Do not click on links or open attachments unless you recognize the sender and know that the content is safe. If you believe that this email is suspicious, please forward to [phishing@dc.gov](mailto:phishing@dc.gov) for additional analysis by OCTO Security Operations Center (SOC).

Good morning –

It is our understanding that, pursuant to D.C. Act 23-328 § 808, the MPD was required to respond to our public records request 2021-FOIA-01634 (attached) by today. I am writing to follow up on the status of our request.

Thank you,

Laura

Laura Hecht-Felella  
George A. Katz Fellow, Liberty & National Security Program  
Brennan Center for Justice at NYU School of Law  
120 Broadway, Suite 1750, New York, NY 10271  
(646) 292-8385 | [hecht-felella@brennan.law.nyu.edu](mailto:hecht-felella@brennan.law.nyu.edu)

---

**From:** Laura Hecht-Felella  
**Sent:** Thursday, February 11, 2021 3:22 PM  
**To:** robert.eckert@dc.gov; latrina.crumlin2@dc.gov; lisa.archie-mills@dc.gov  
**Cc:** Sahil Singhvi <[singhvis@brennan.law.nyu.edu](mailto:singhvis@brennan.law.nyu.edu)>; Rachel Levinson-Waldman <[levinsonr@brennan.law.nyu.edu](mailto:levinsonr@brennan.law.nyu.edu)>  
**Subject:** RE: Acknowledgement Letter 2021-FOIA-01634

Dear Mr./Ms. Crumlin,

I hope this email finds you well. The Brennan Center is in receipt of your December 16, 2020 response regarding our FOIA request number 2021-FOIA-01634. The Metropolitan Police Department (MPD) claimed a Covid-19 extension pursuant to D.C. Act 23-328 § 808 that allowed it to extend the response deadline for this request until the public health emergency ended.

However, [the FOIA Tolling Emergency Amendment Act of 2020](#) (effective December 22, 2020) requires the MPD to provide a response to our request within 45 days (except Saturdays, Sundays, and legal public holidays) of the end of the “Initial COVID-19 closure,” which was on January 15, 2021.

Therefore, we request that MPD respond to our request by **March 24, 2021** and “either make the requested public record accessible or notify the person making such request of its determination not to make the requested public record or any part thereof accessible and the reasons therefor.”

Please do not hesitate to contact me with further questions at (646) 292-8385. Thank you for your attention to this matter.

Thank you,

Laura

Laura Hecht-Felella  
George A. Katz Fellow, Liberty & National Security Program  
Brennan Center for Justice at NYU School of Law  
120 Broadway, Suite 1750, New York, NY 10271  
(646) 292-8385 | [hecht-felella@brennan.law.nyu.edu](mailto:hecht-felella@brennan.law.nyu.edu)

---

**From:** [latrina.crumlin2@dc.gov](mailto:latrina.crumlin2@dc.gov) <[latrina.crumlin2@dc.gov](mailto:latrina.crumlin2@dc.gov)>  
**Sent:** Wednesday, December 16, 2020 12:28 PM  
**To:** [sahil.singhvi@nyu.edu](mailto:sahil.singhvi@nyu.edu)  
**Cc:** [robert.eckert@dc.gov](mailto:robert.eckert@dc.gov); [latrina.crumlin2@dc.gov](mailto:latrina.crumlin2@dc.gov); [lisa.archie-mills@dc.gov](mailto:lisa.archie-mills@dc.gov)  
**Subject:** Acknowledgement Letter 2021-FOIA-01634

Dear Mr./Mrs. Singhvi,

This office is in receipt of your Freedom of Information Act (FOIA) request. Your FOIA request number is 2021-FOIA-01634 and your assigned FOIA Specialist is **Robert Eckert**.

If you have any questions regarding your request, please contact your assigned FOIA Specialist at (202) 727-3721. For ease of reference, we ask that you have your FOIA Request Number available when you contact our office.

Please know, pursuant to D.C. Official Code § 2-532(c), we have 15 business-days, subject to the possibility of a ten (10) business day extension to respond to the request as of the date of receipt.

Be advised, if your request is for Body Worn Camera (BWC) footage, D.C. Code § 2-532(c) allows 25 business days subject to the possibility of 15 working-day extension, to respond to the request as of the date of receipt.

**COVID-19 Notification**

Pursuant to section 808 of the Coronavirus Support Congressional Review Emergency Amendment Act of 2020, **effective June 9, 2020**, D.C. Act 23-328, all FOIA deadlines may be extended during a period of time for which the Mayor has declared a public health emergency. Pursuant to this provision, we have claimed an extension of the time in which to provide a response to your request.

Regards,

Latrina Crumlin  
Staff Assistant, FOIA  
Metropolitan Police Department

300 Indiana Ave NW, RM 4153  
Washington, DC 20001

# Exhibit C

---

**From:** Eckert, Robert (MPD) <robert.eckert@dc.gov>

**Sent:** Thursday, September 30, 2021 3:52 PM

**To:** Laura Hecht-Felella <hecht-felella@brennan.law.nyu.edu>

**Cc:** Eckert, Robert (MPD) <robert.eckert@dc.gov>

**Subject:** Final Response in Process - FOIA Request No. 2021-FOIA-01634, from Laura Hecht-Felella (Brennan Center for Justice)

**September 30, 2021**

**Laura Hecht-Felella**  
**George A. Katz Fellow**  
**(submitted via Sahil Singhvi)**  
**Liberty and National Security Program**  
**Brennan Center for Justice at NYU School of Law**  
**hecht-felella@brennan.law.nyu.edu**

**FOIA Request No. 2021-FOIA-01634**

**Dear Ms. Hecht-Felella:**

**This is in response to the above-referenced Freedom of Information Act (FOIA) request for a variety of information as reflected below, along with response information received through the search for responsive records.**

"1. Policies Governing Use: Any and all department-wide or unit-specific policies, procedures, regulations, protocols, manuals, or guidelines related to: a. the use of social media monitoring by police department employees including, but not limited to, for the purposes of conducting a criminal investigation, undertaking situational awareness activities, monitoring current or anticipated gatherings, or otherwise viewing or gathering information about individuals; b. the authorization, creation, use, and maintenance of fictitious/undercover online personas; c. the collection and maintenance of location data from social media platforms and/or applications; or d. the retention, analysis, or sharing of data collected via social media."

**The following references are responsive to this FOIA request, which may be located on the MPD website (<https://mpdc.dc.gov/page/written-directives-general-orders>): SO-13-04 Investigative Support Unit; SO-14-05 CIC Traffic Desk; SO-16-06 Social Media Checks for Background; SOP 16-01 Handling First Amendment Assemblies; ISS CRS Social Media Policy; ISS Social Media Training; and, ISS Social Media Procedures.**

**Also located were the attached: ISS CRS Social Media Policy; ISS Social Media Training; ISS Social Media Procedures, Memorandum of Understanding (MOU) Between the District of Columbia (DC) Homeland Security and Emergency Management Agency (HSEMA) and the Metropolitan Police Department (MPD); Emergency Disclosure and Preservation Requests; and, DCR (Crime Statistics) 01/01/2013 - 12/21/2020.**

**No records reflecting fictitious online personas/accounts were located.**

2. Recordkeeping: Any and all recordkeeping, logs, or digests reflecting the use of social media monitoring, or searches of social media for purposes including criminal investigations, situational awareness, event planning, or public safety.

**A search located no records of logs reflecting social media searches for the purpose of criminal investigations, situational awareness, event planning, or public safety. Analysts and other MPD members often rely on open-source (publicly available) social media searches to find information about planned demonstrations or criminal activities.**

"3. Purchase Agreements and Orders: Any and all records reflecting a contract or agreement to purchase, acquire, use, test, license, or evaluate any product or service developed by any company providing third-party social media monitoring services, including, but not limited to, Dataminr, Geofeedia, Snaptrends, Firestorm, Media Sonar, Social Sentinel, or Dunami."

**No records of contracts for social media monitoring applications were located. The MPD does have access to Dataminr, an application purchased by the Office of the Chief Technology Officer (OCTO)/Homeland Security Emergency Management Agency (HSEMA)/National Technology Information Center (NTIC). The MPD has access through the attached memorandum of understanding (MOU) with NTIC. The NTIC provides alerts from Dataminr's First Alert to the Joint Strategic and Tactical Analysis Command Center (JSTACC) management. Dataminr's First Alert uses technology to detect breaking events and emerging risks from open-source social media in real time.**

"4. Social Media Account Information from Civilians: Any and all records reflecting: a. interactions with civilians in which police department employees requested information about the civilian's social media account information, including, but not limited to, a username, identifier, handle, linked email, or password; or b.



communications conducted on social media platforms between uniformed or undercover police department employees and civilians, including, but not limited to, direct messages, group messages, chat histories, comments, or "likes." But excluding communications conducted as part of ongoing investigations and communications appearing on a page or account operated by the MPD and bearing the MPD's name, insignia, or other indicia of ownership or control."

**This is not something maintained in a database, but would be part of a criminal investigation, and would require research, which is not required under the FOIA. Additionally, as mentioned above, JSTACC members do not create fictitious online personas or interact in an undercover capacity on social media platforms.**

"5. Use for Criminal Investigations: Any and all records reflecting the number of criminal investigations in which social media research has been used, the number of criminal investigations in which fictitious/undercover online personas have been used, the nature of the offenses charged in those investigations, and the number of those investigations that resulted in arrests and/or prosecutions."

**The MPD has no records responsive to this portion of the request.**

"6. Use for Purposes Other Than Criminal Investigations: Any and all records reflecting the number of circumstances in which social media was used to collect information about individuals for purposes other than criminal investigations or background checks for police department employment, including regarding protest activity, as well as the number of such matters in which an individual or group was charged with a crime."

**No records responsive to this item of the request were located.**

**Situational Awareness - The MPD utilizes TweetDeck, which is a free social media dashboard application for management of Twitter accounts. Originally an independent application, TweetDeck was subsequently acquired by Twitter Inc. and integrated into Twitter's interface. It is normally used to monitor trending topics in real-time 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. Real-time monitoring is not tracked as it is all open source (publicly available data). Additionally, MPD's Intelligence Branch completes a daily demonstration report which provides a daily list of known demonstrations. It's compiled based on known permit applications through MPD, USPP, etc. and open media searches for demonstrations occurring in DC.**

**As far as First Amendment demonstrations - MPD does not keep "files" on individuals involved in protest/demonstration activity, to include social media accounts, unless MPD has been authorized to conduct an investigation as outlined by First Amendment activities as required by the Police Investigations Concerning First Amendment Activities Act of 2004 (the Act), D.C. Code § 5-333 et seq.**

"7. Audits: Any and all records of, or communications regarding, audits or internal reviews of the Department's use of social media monitoring for the purpose of investigations, situational awareness, event planning, intelligence, or public safety, including, but not limited to, records reflecting any disciplinary actions, warnings, or proceedings in response to an employee's use of social media."

**No records responsive to this portion of the request were located. Social media inquiries by JSTACC are open source (publicly available).**

"8. Training Materials: Any and all training documents, including drafts, discussing social media monitoring, including, but not limited to, PowerPoint presentations, handouts, manuals, or lectures."

**Please see the attached the following training material regarding social media investigations. These are given internally to JSTACC members, as well as in investigator and district intelligence officer training: 081920 Investigator Training - Emergency Disclosures ISS Social Media Training Updated.**

“9. Legal Justifications: Any and all records reflecting the legal justification(s) for social media monitoring, including, but not limited to, memos, emails, and policies and procedures.”

**No responsive records were located.**

“10. Formal Complaints, Freedom of Information Requests, and Legal Challenges: Any and all records reflecting formal complaints, FOIA requests, or legal challenges regarding the Department’s use of social media monitoring, including, but not limited to, those complaints or legal challenges made by civilians, nonprofit groups, or companies.”

**A search located no records of formal complaints or legal challenges regarding social media monitoring.**

“11. Federal Communications: Any and all records reflecting any communications, contracts, licenses, waivers, grants, or agreements with any federal agency concerning the use, testing, information sharing, or evaluation of social media monitoring products or services. This includes, but is not limited to, records reflecting communications regarding information sharing between MPD and federal law enforcement agencies, such as the FBI, Secret Service, Park Police, ATF, DEA, Bureau of Prisons, U.S. Marshals Service, Capitol Police, Department of Homeland Security’s CBP and Border Patrol units, in response to protests in June 2020.”

**A search located no records responsive records; however, the attached MOU with the DC HSEMA, referenced in the response to No. 1, is attached.**

“12. Nondisclosure Agreements: Any and all records regarding the MPD’s nondisclosure or confidentiality obligations in relation to contracts or use agreements with third-party vendors of social media monitoring products or services.”

**As previously mentioned, MPD does not have any contracts with any social media vendors. Therefore, we would not have any nondisclosure agreements.**

13. Vendor Communication: Any and all records reflecting interactions with any third-party vendors concerning social media monitoring products or services, including, but not limited to, sales materials, licensing agreements, communications, memorandums, and emails relating to those products.

**No responsive records were located.**

**I have determined to withhold portions of the released records under DC Official Code § 2-534 (a)(2) and (a)(3) because their release would constitute a clearly unwarranted invasion of personal privacy. The withheld material includes names/personal identifiers and other personal privacy information, including that which would lead to the identity of individuals.**

**Please know that, under D.C. Official Code § 2-537 and 1 DCMR § 412, you have the right to appeal this letter to the Mayor or to the Superior Court of the District of Columbia. If you elect to appeal to the Mayor, your appeal must be in writing and contain “Freedom of Information Act Appeal” or “FOIA Appeal” in the subject line of the letter, as well as, on the outside of the envelope. The appeal must include (1) a copy of the original request; (2) a copy of any written denial; (3) a statement of the circumstances, reasons, and/or arguments advanced in support of disclosure; and (4) a daytime telephone number, an e-mail and/or U.S. mailing address at which you can be reached.**

**The appeal must be mailed to: The Mayor’s Office of Legal Counsel, FOIA Appeal, 1350 Pennsylvania Avenue, N.W., Suite 407, Washington, D.C. 20004. Electronic versions of the same information can instead be e-mailed to the Mayor’s Office of Legal Counsel at [foia.appeals@dc.gov](mailto:foia.appeals@dc.gov). Further, a copy of all appeal materials must be forwarded to the Freedom of Information Officer of the involved agency, or to the agency head of that agency, if there is no designated Freedom of Information Officer there. Failure to follow these administrative steps will result in delay in the processing and commencement of a response to your appeal to the Mayor.**

**Sincerely,  
Bob Eckert  
FOIA Specialist  
Freedom of Information Act Office  
Metropolitan Police Department  
[Robert.eckert@dc.gov](mailto:Robert.eckert@dc.gov)  
“Excellence is transferable.”**

# Exhibit D

**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]

# Exhibit E



**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.

[REDACTED]

[REDACTED]

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 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 F



# SOCIAL MEDIA

INVESTIGATIVE SUPPORT SECTION

JOINT STRATEGIC & TACTICAL ANALYSIS COMMAND CENTER

## METROPOLITAN POLICE DEPARTMENT

WASHINGTON, D.C.

**PETER NEWSHAM**  
CHIEF OF POLICE

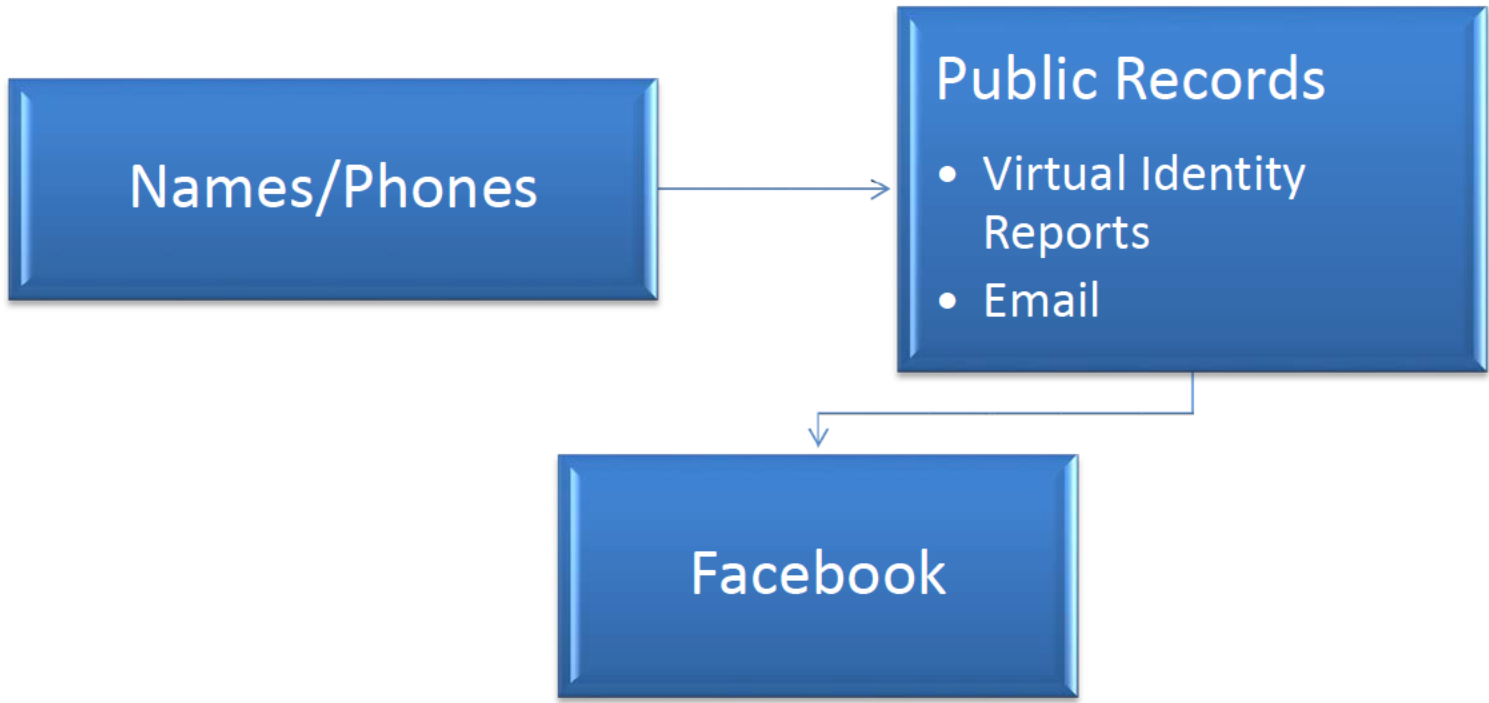


- Provide insight on how the Investigative Support Section (ISS) provides open source intelligence for investigative purposes
  - Old vs New procedures
- Techniques
- Challenges & Solutions
- Examples/Success stories



- 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.





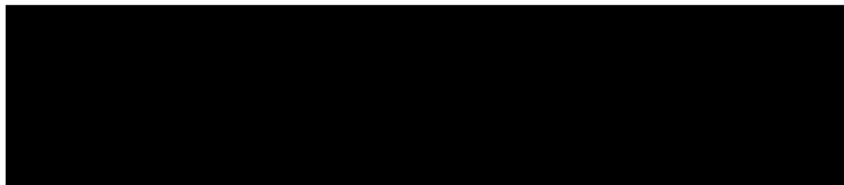
**Barely scratching the surface**

Robbery Arrestee:



Accurint:

Virtual Identity Report



Facebook:



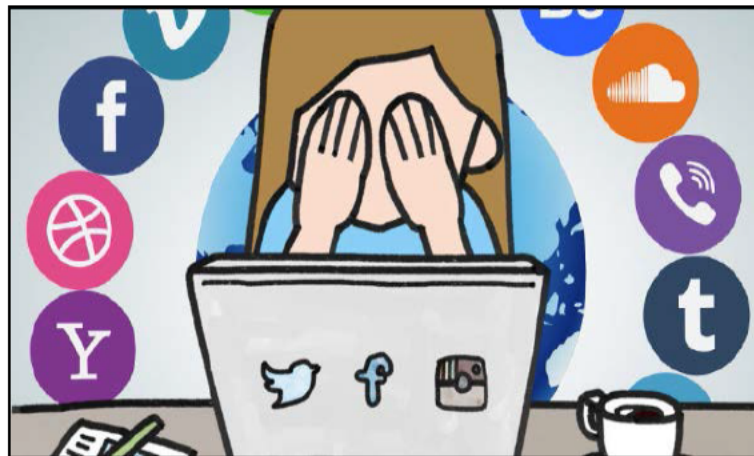
We couldn't find anything for [REDACTED]

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

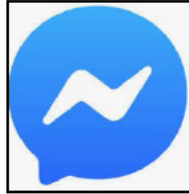


Use other public records (TLO) to find any  
possible emails, phones, relatives, etc.



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

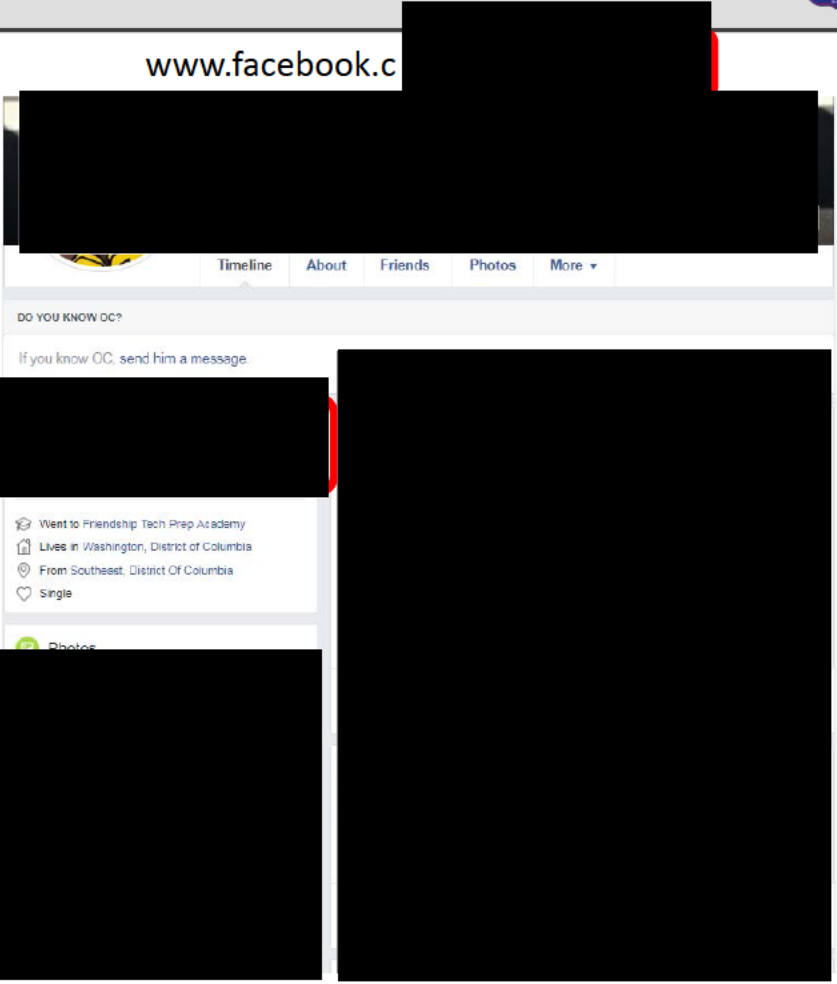
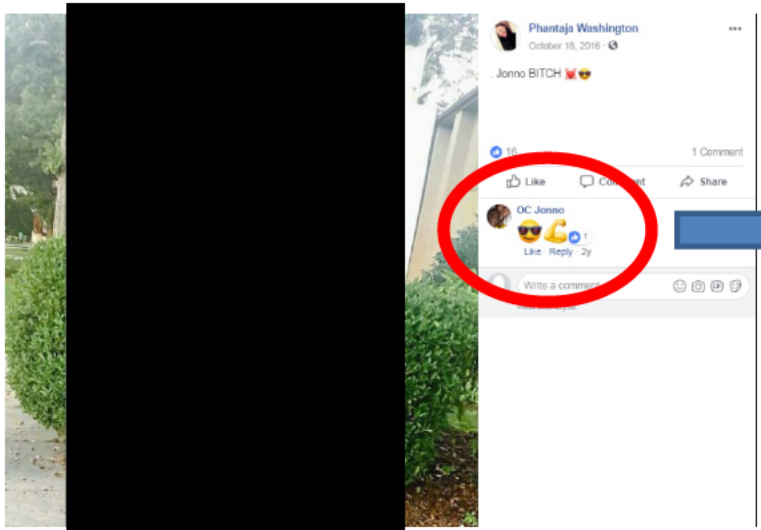
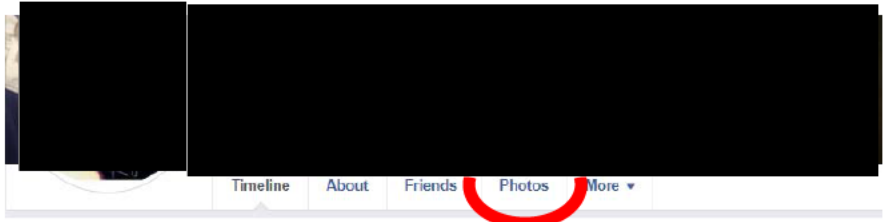
# SOCIAL MEDIA: RESOURCES



# 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

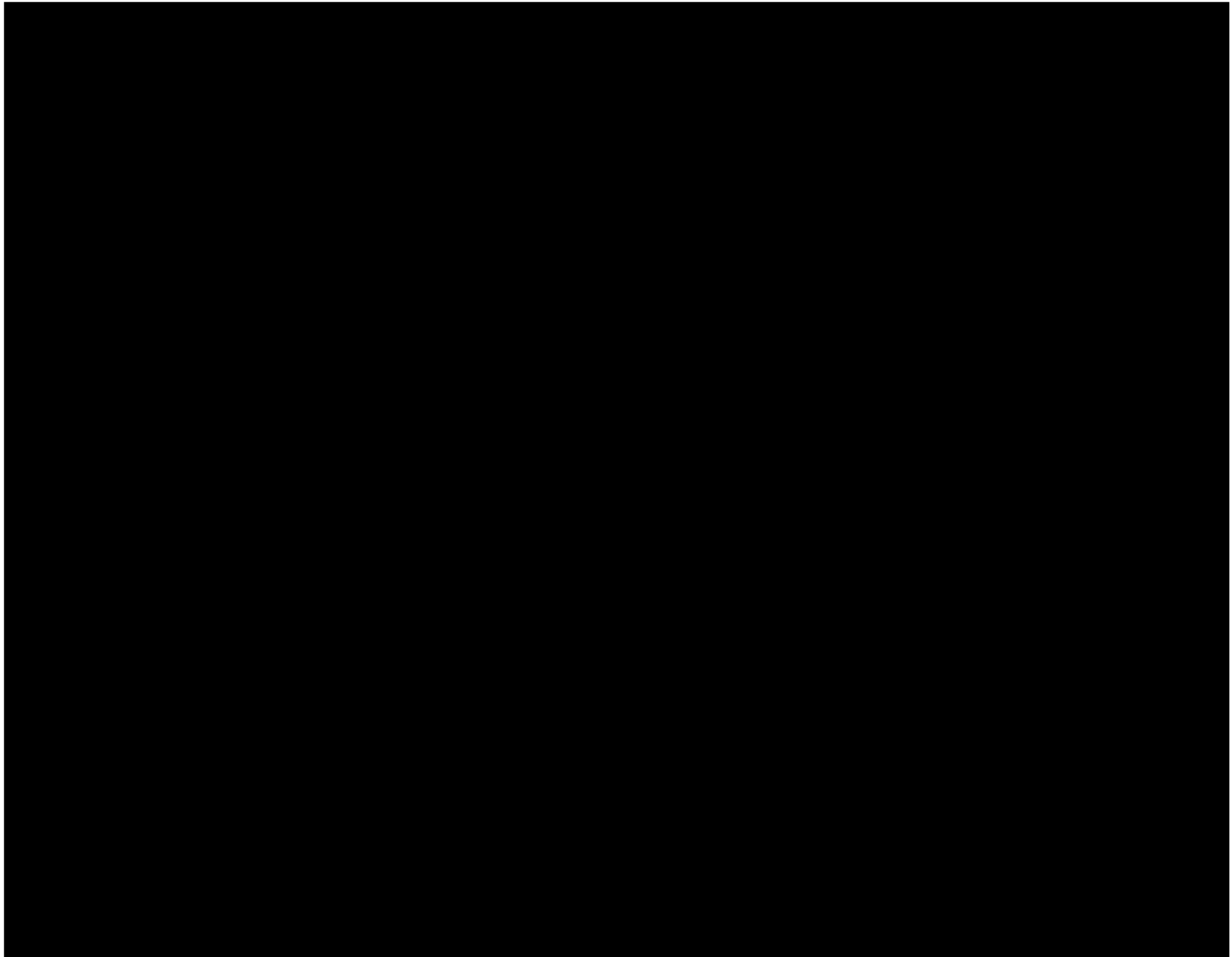




www.instagram.co

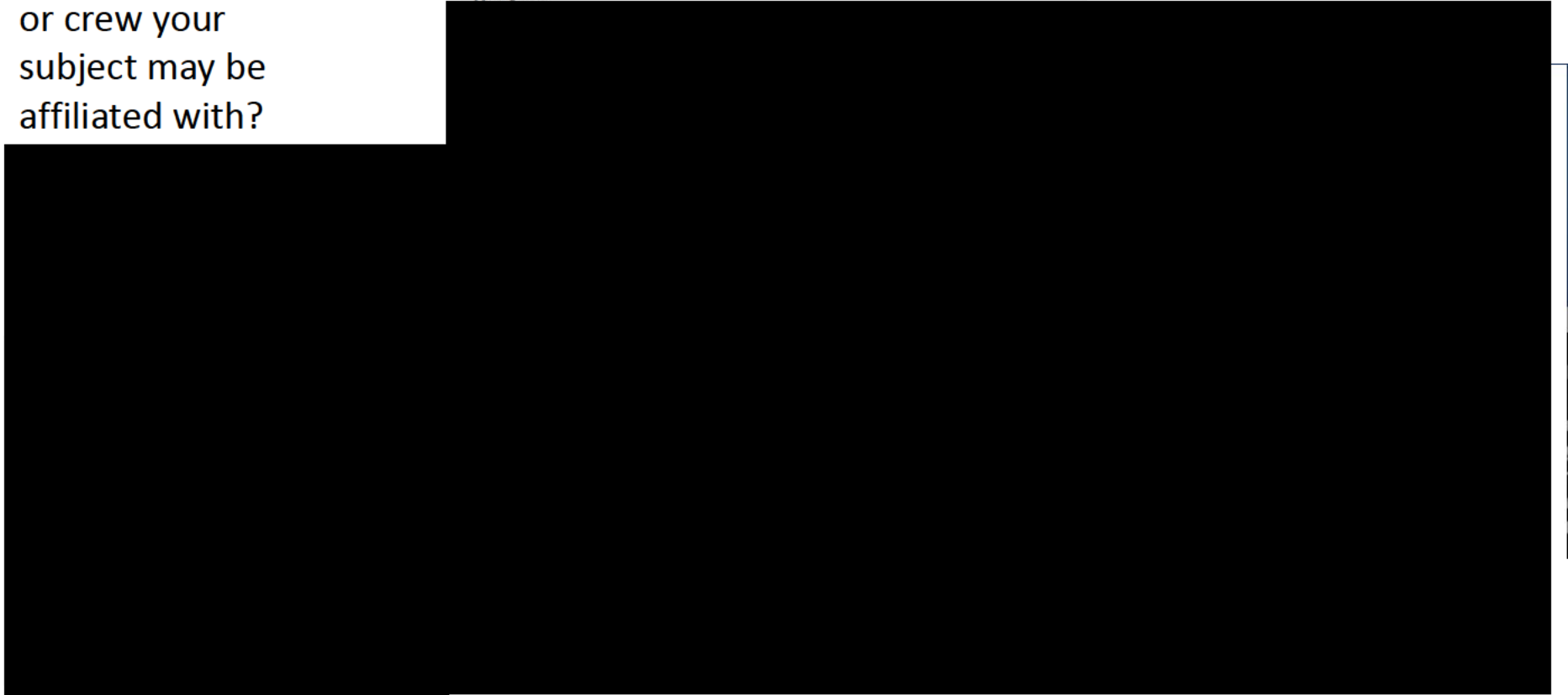


www.instagram.com



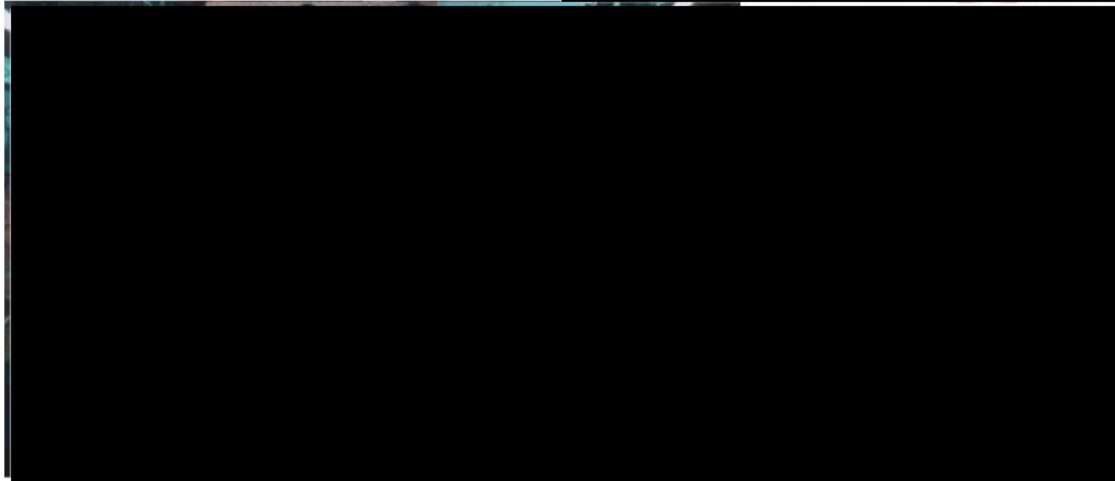
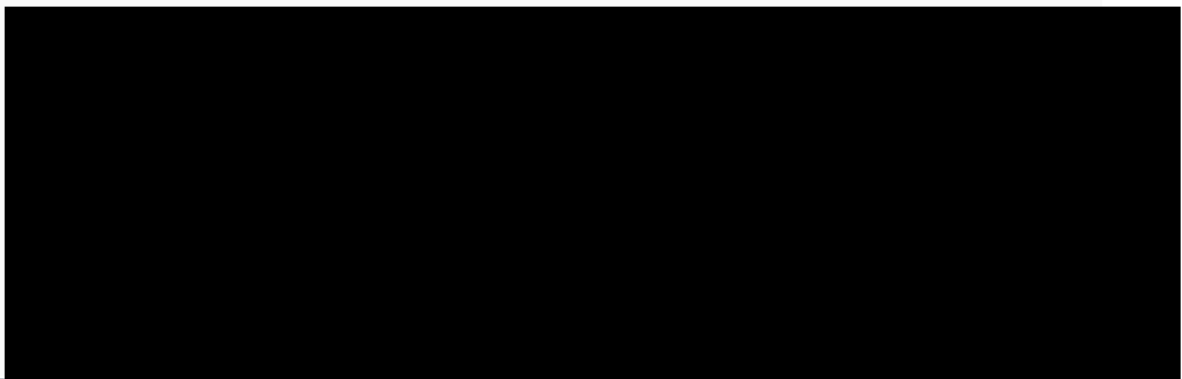
# INSTAGRAM

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



# INSTAGRAM CONT'D.

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

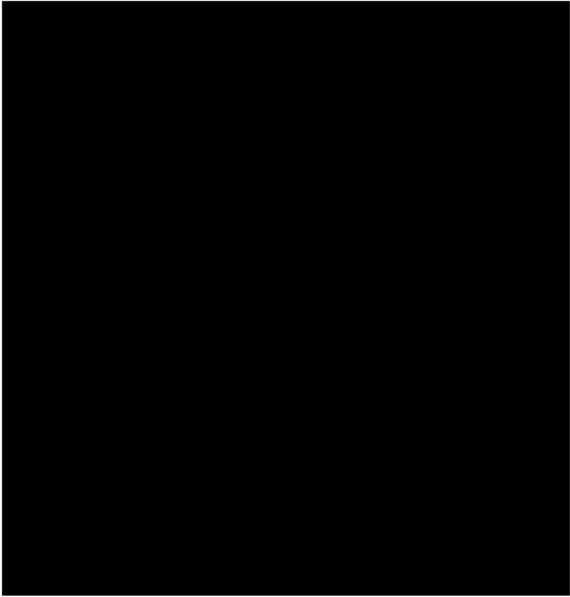
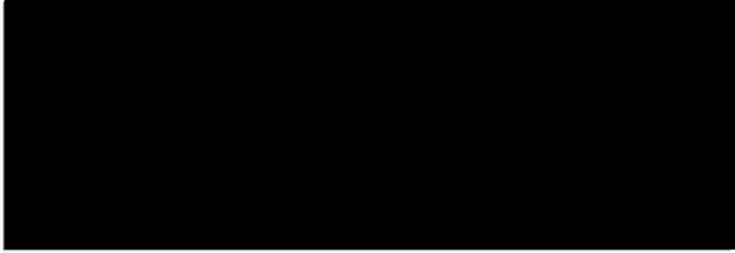


Based on the profile bio and photos it appears [redacted] and [redacted] may be keywords associated with subjects from Simple City

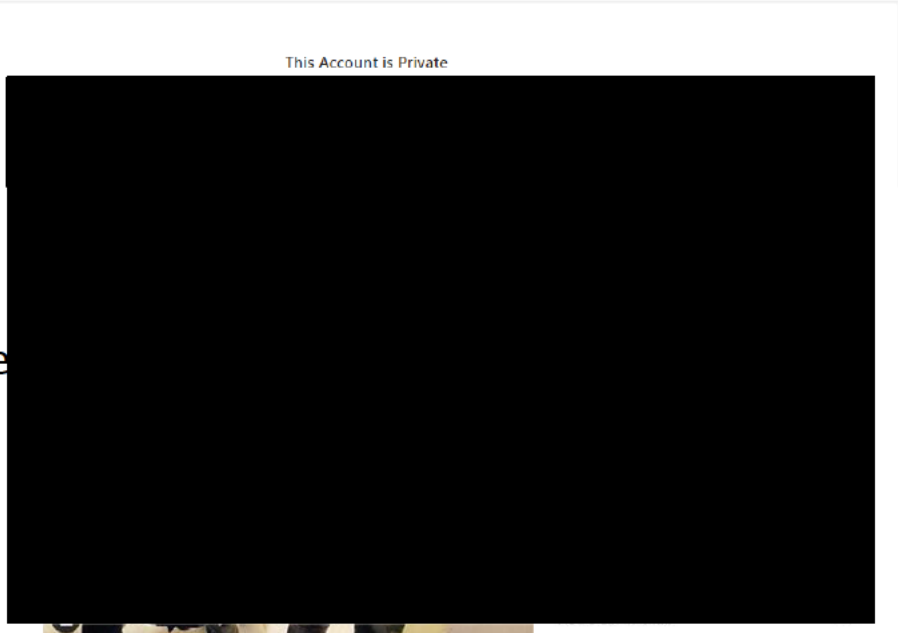
# INSTAGRAM CONT'D

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

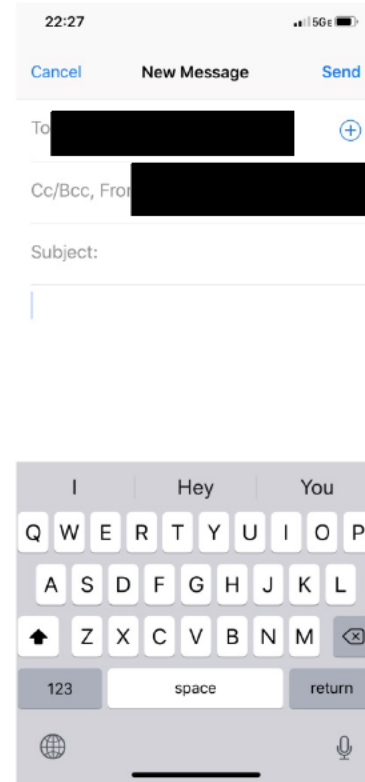
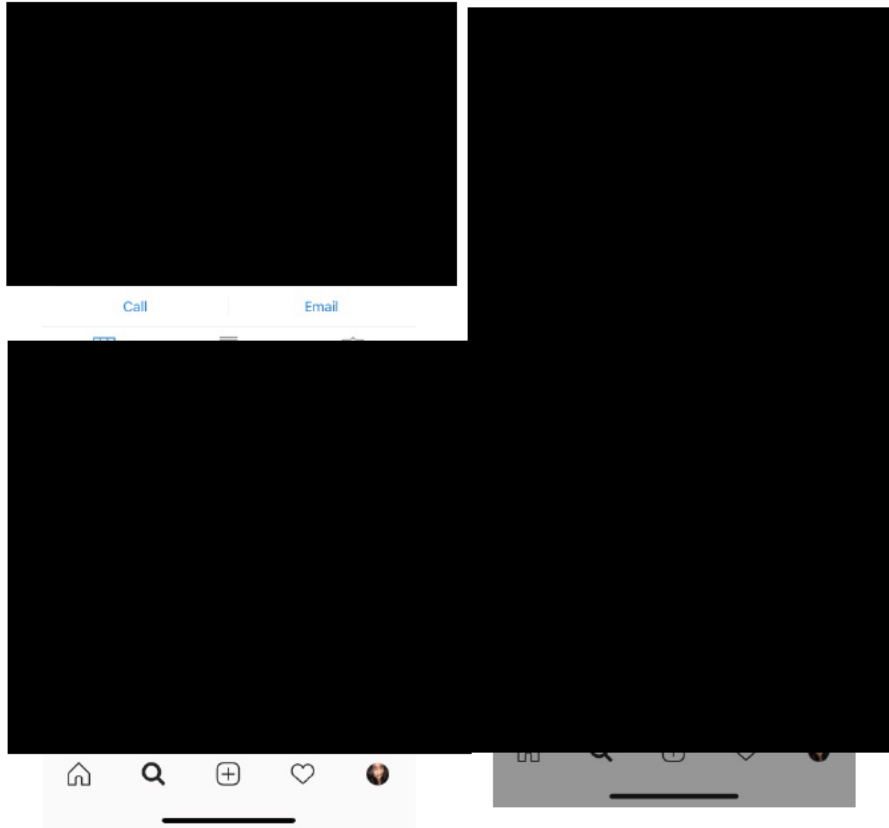
[redacted] account is private, how can we combat it?



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

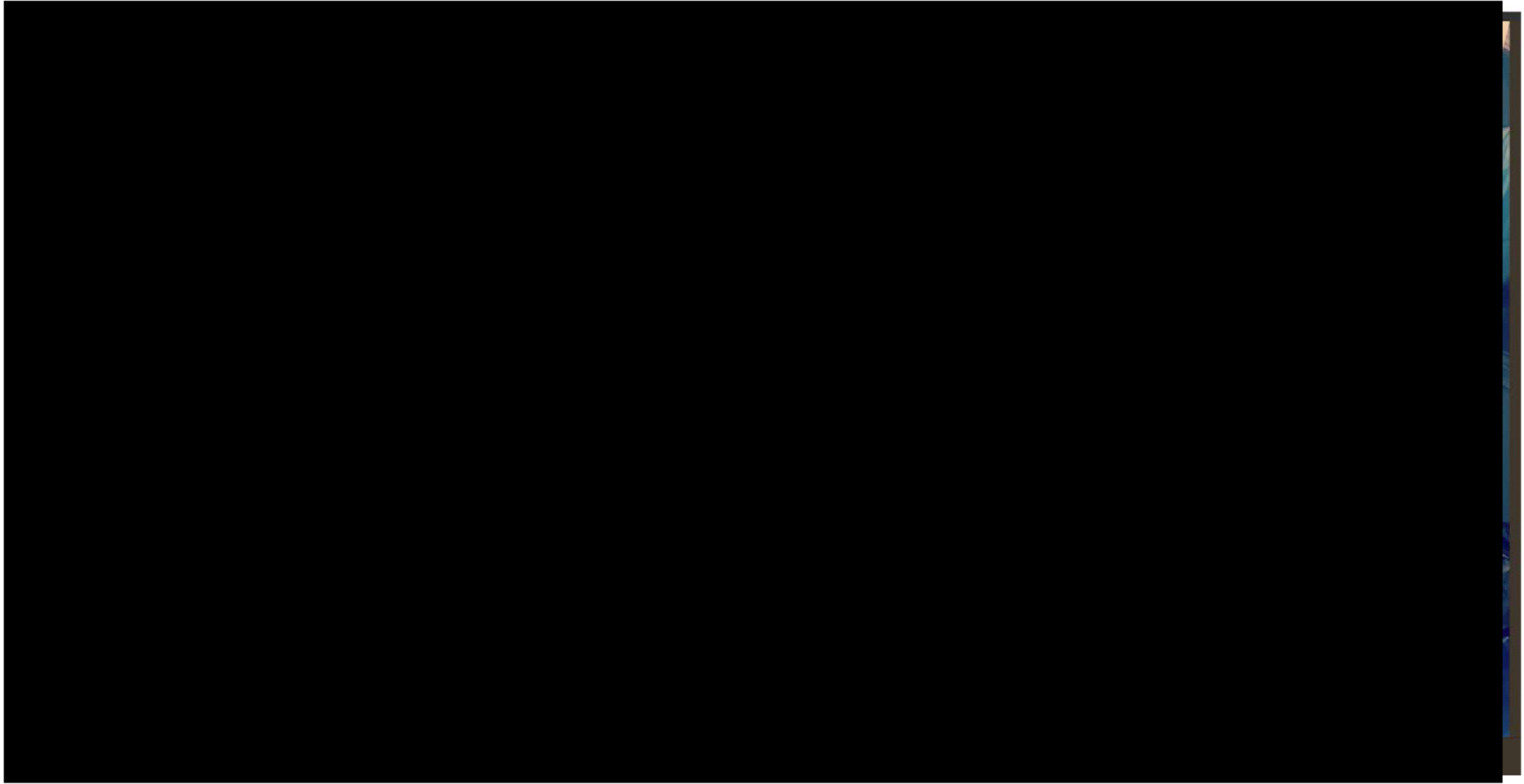


# INSTAGRAM CONT'D





**TWITTER**



# SOCIAL MEDIA: TARGETED SEARCHES

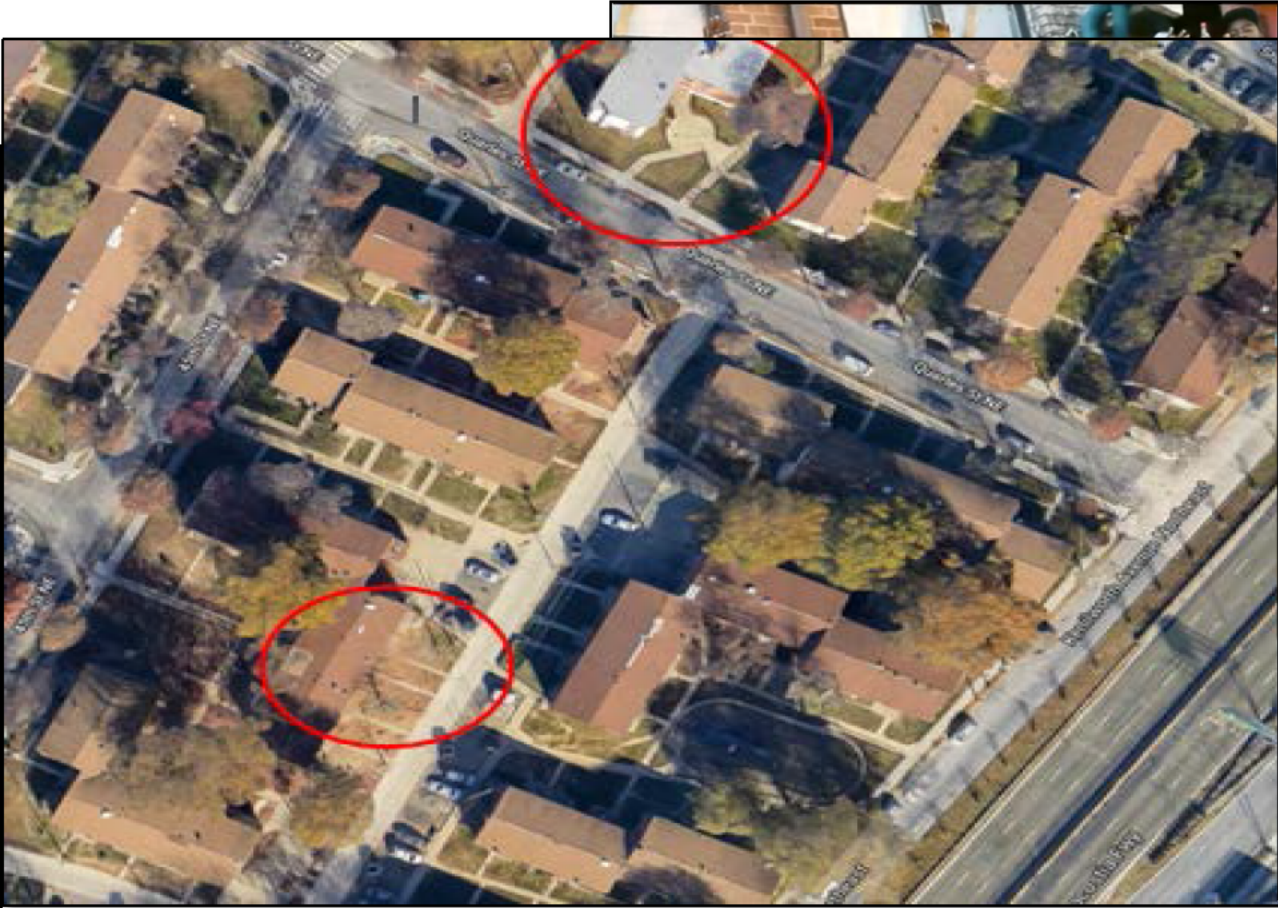


- Social Media drill downs on homicides and high profiles cases/individuals of interest
  - Quick turnaround time for requests
    - Around the clock requests/communication needed between shifts
  - Building out information on hashtags, possible retaliation/crew beefs, relatives/associates
  - Information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

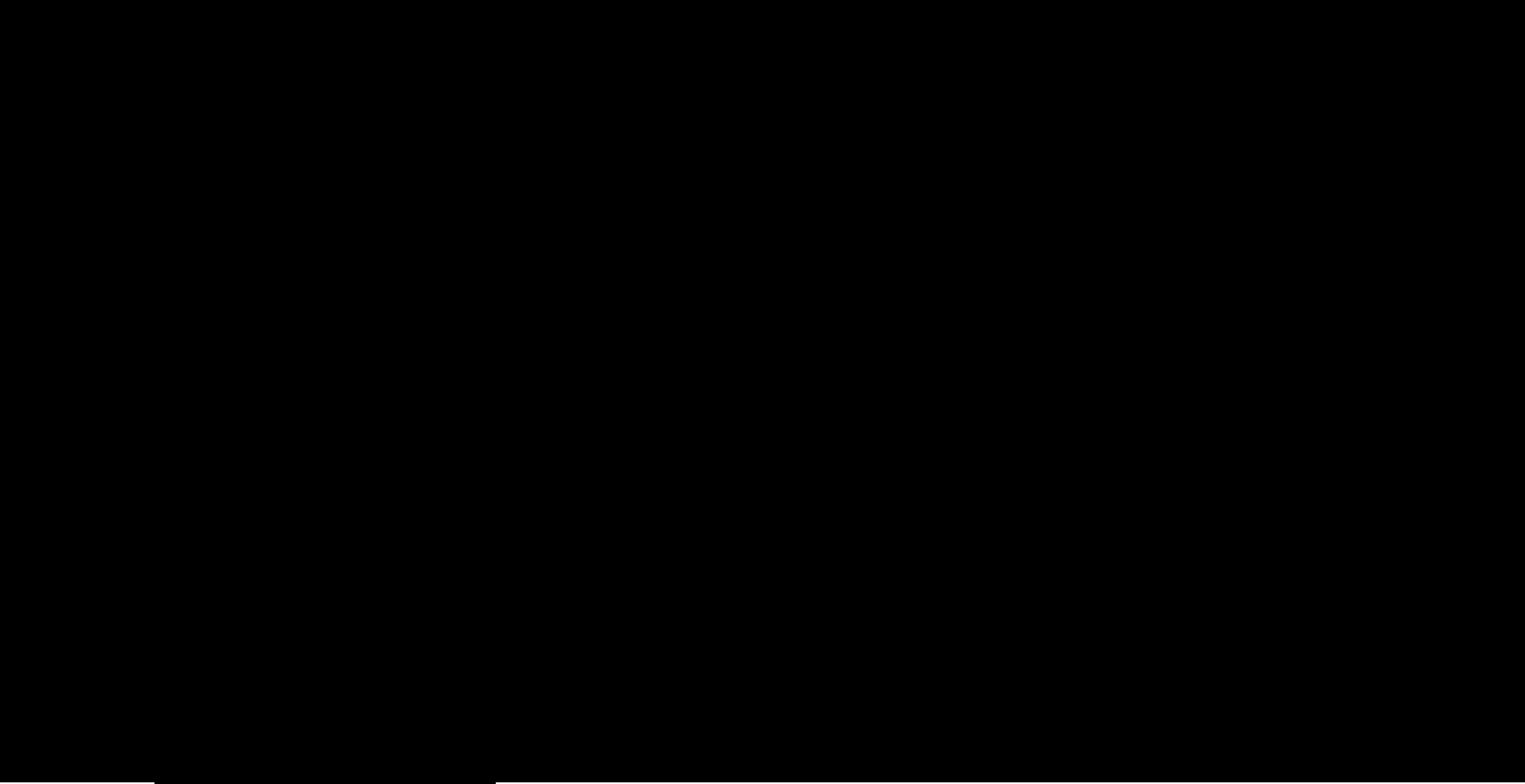




# SOCIAL MEDIA: TARGETED SEARCHES – YOUTUBE/INSTAGRAM



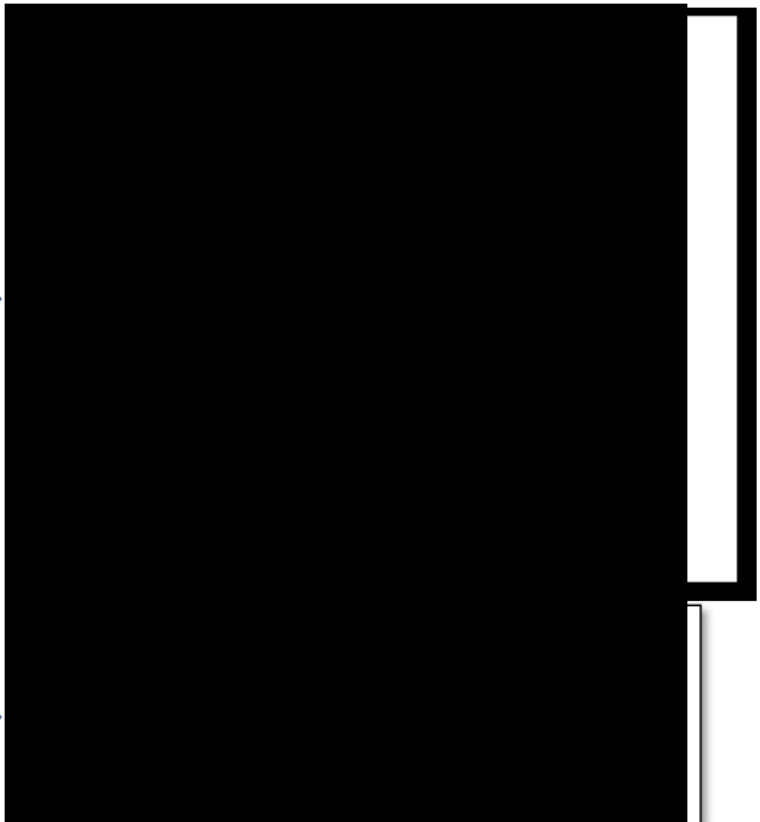
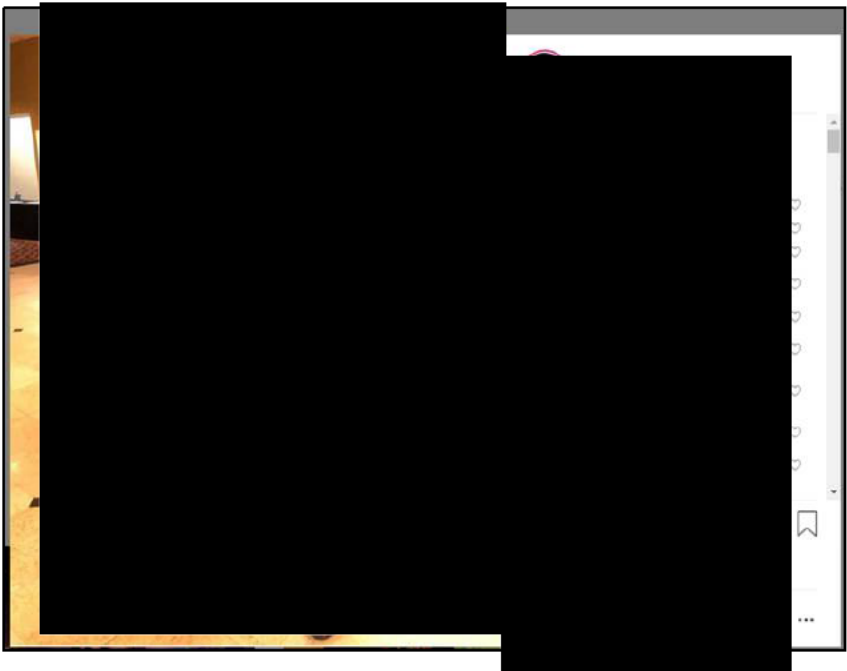
# SOCIAL MEDIA: TARGETED SEARCHES – YOUTUBE/INSTAGRAM

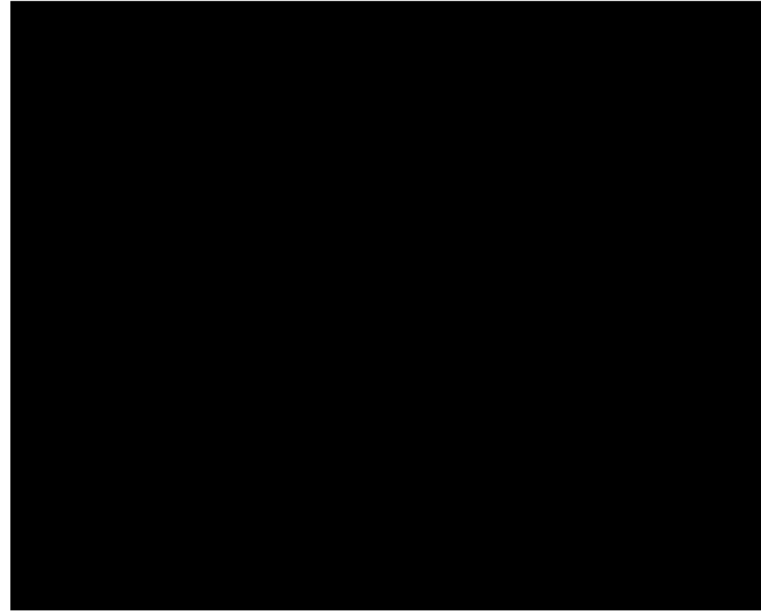
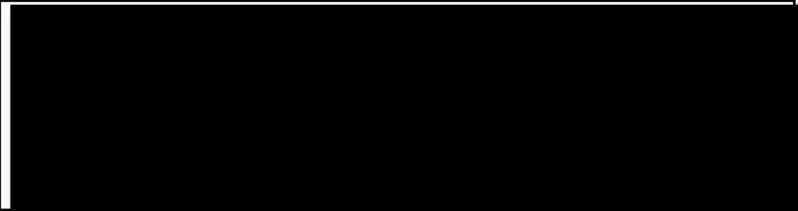


# SOCIAL MEDIA: TARGETED SEARCHES - EXAMPLE

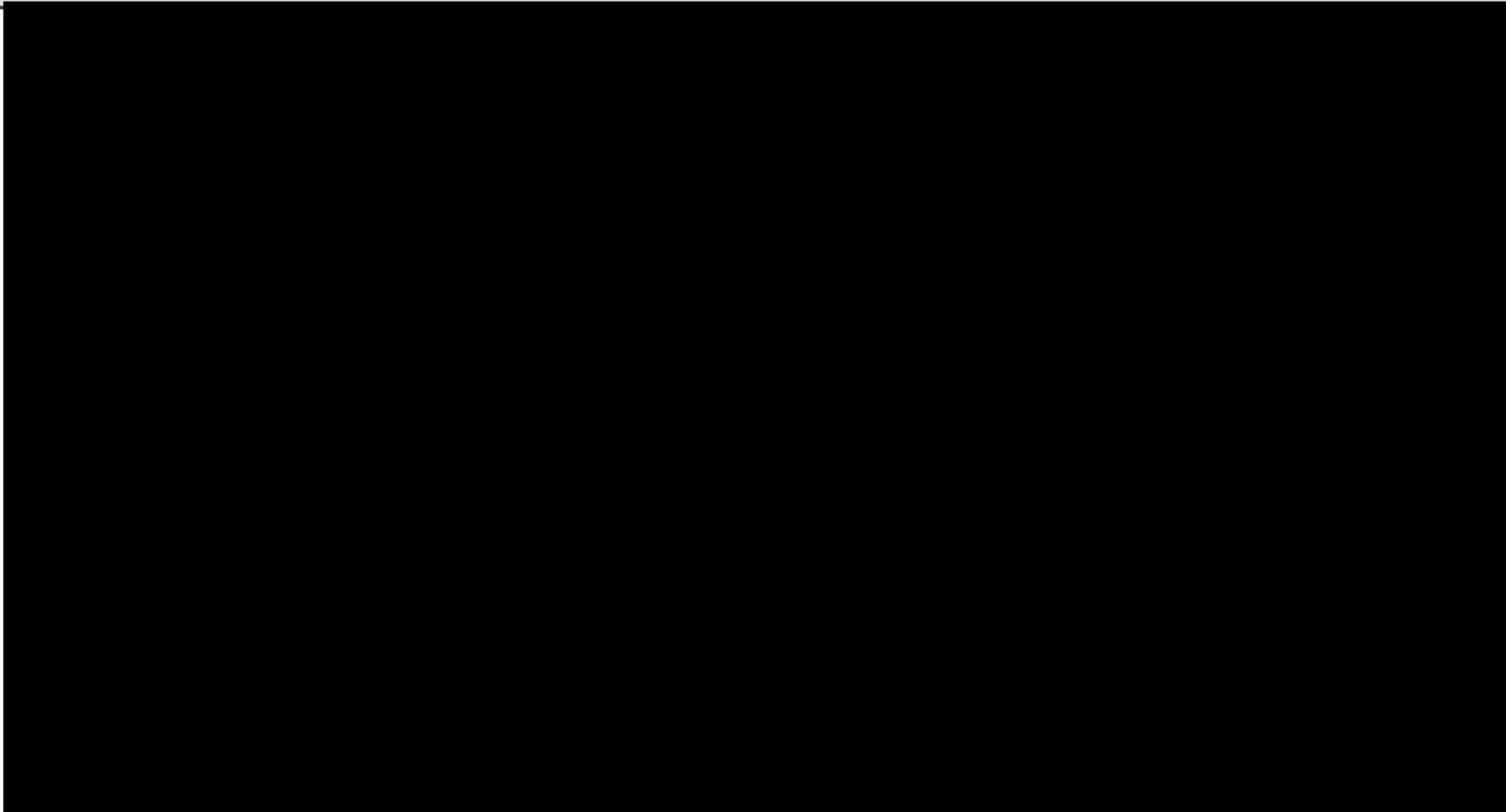
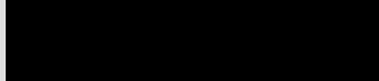
Post homicide follow-up of *validated* [REDACTED]

- 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', followed by the tagline 'Best Instagram story viewer! You can watch Instagram stories anonymously and quickly without the need to log in or having account.' Below this is an advertisement for Google with buttons for 'Stop seeing this ad' and 'Why this ad?'. At the bottom, there is a search bar labeled 'Enter Instagram username' and a 'Search' button. A dark grey navigation bar on the left contains 'Home' and 'Download Stories'.

**Start Download**  
View PDF & Download PDF Converter Guru

## Instagram Downloader

INSTADP

## Instdp search profile pictures

Search and download Instagram profile pictures or stories

INSTADP STORIES

---

🔍 Search username

# 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

s

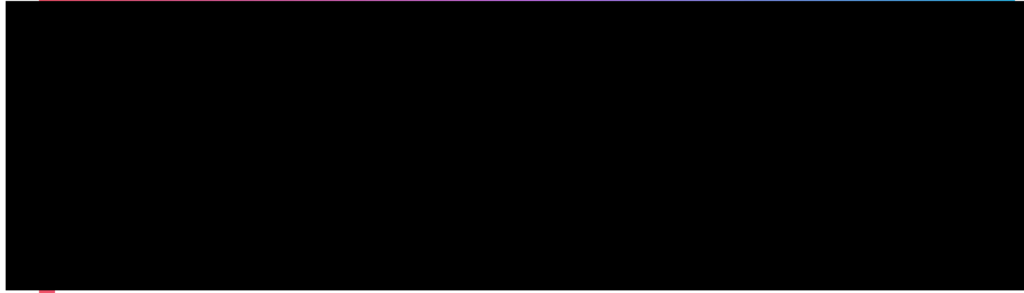


# CHALLENGES: SEARCH RESTRICTIONS STORIESDOWN

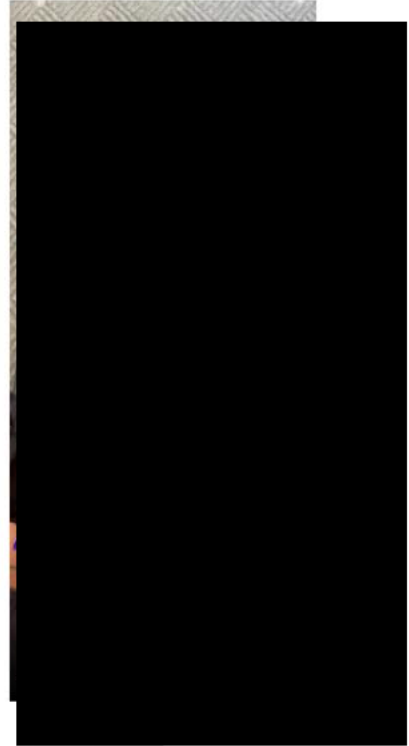
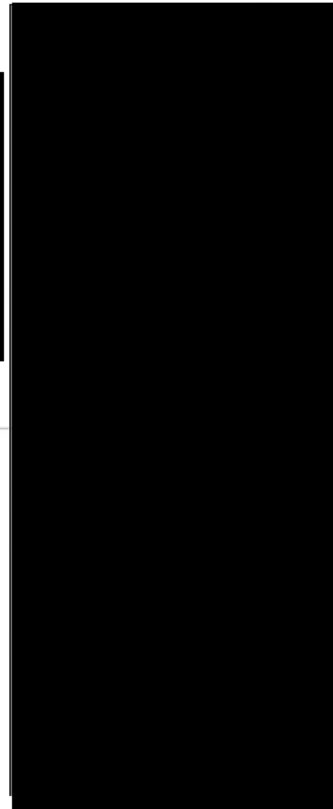


[HOMEPAGE](#) [BLOG](#) [REMOVE CONTENT](#) [CONTACT US](#)

*Stories*



*Posts*



5 hours and 42 minutes ago

# CHALLENGES: SEARCH RESTRICTIONS W3TOYS



**Start Download**  
View PDF & Download PDF Converter Guru

Inst.  
Instagar

## Instagram Downloader

[https://www.instagram.com/p/B\\_Av\\_YgH1ge/](https://www.instagram.com/p/B_Av_YgH1ge/)

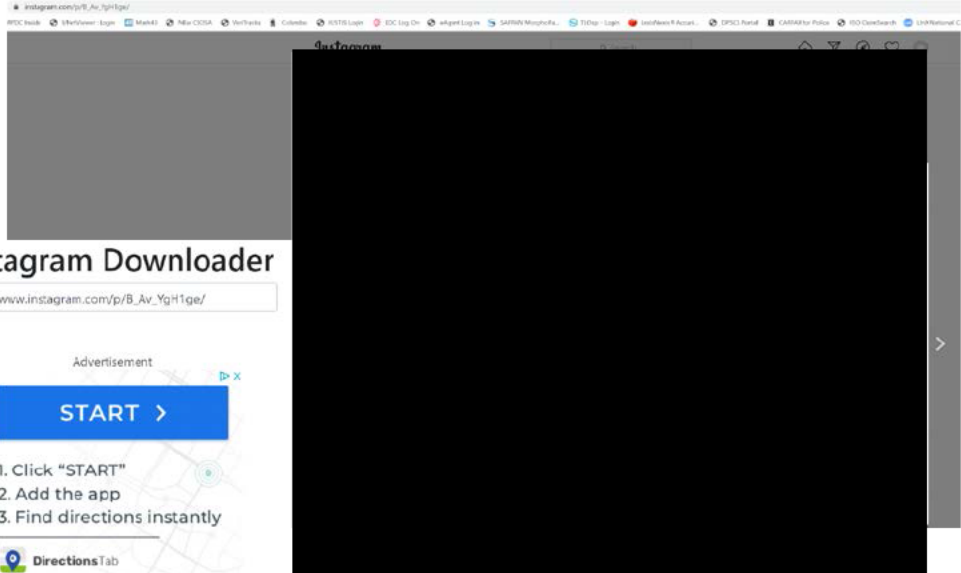
Advertisement

**START >**

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

Directions Tab

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

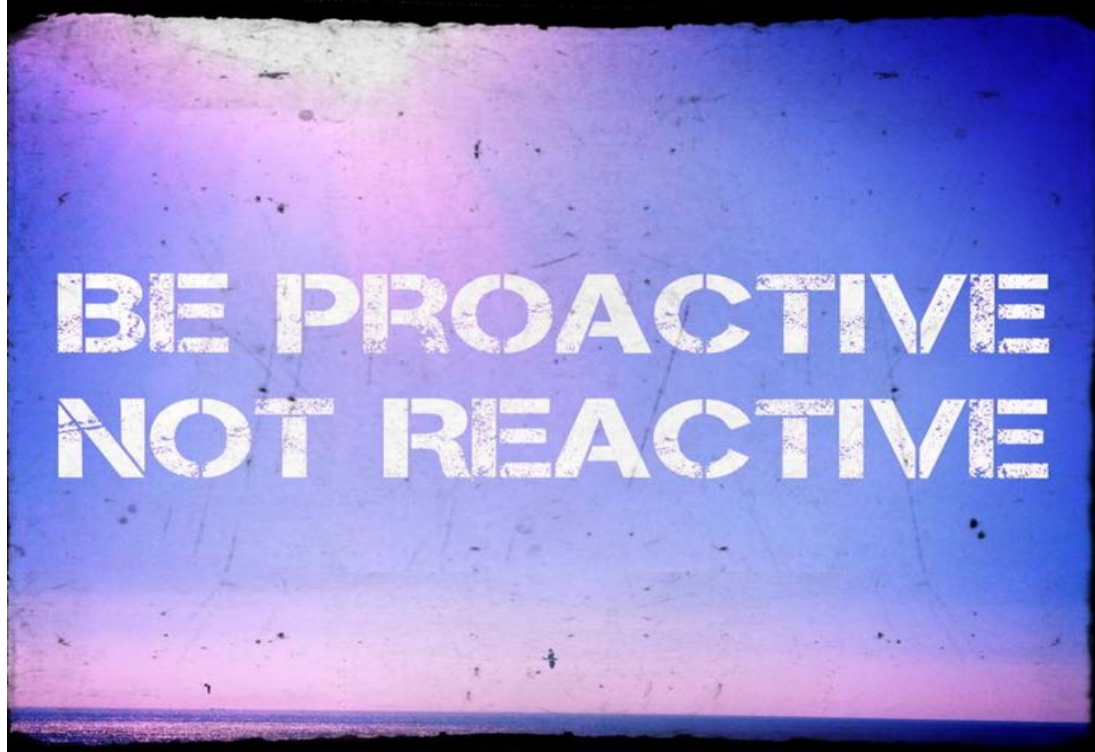
#tagboard

Lullar.com

SnapBird

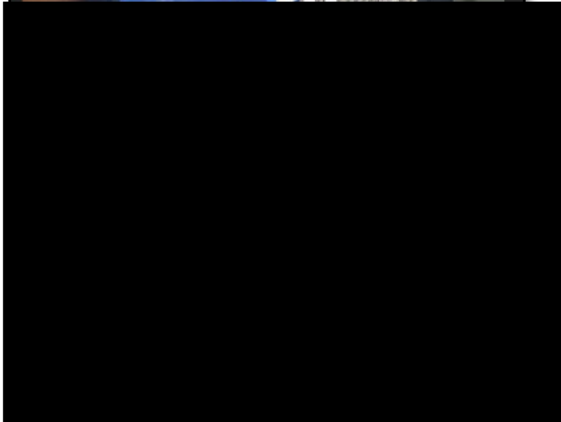
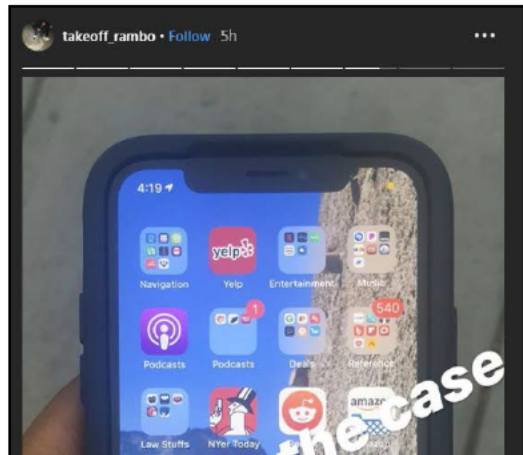
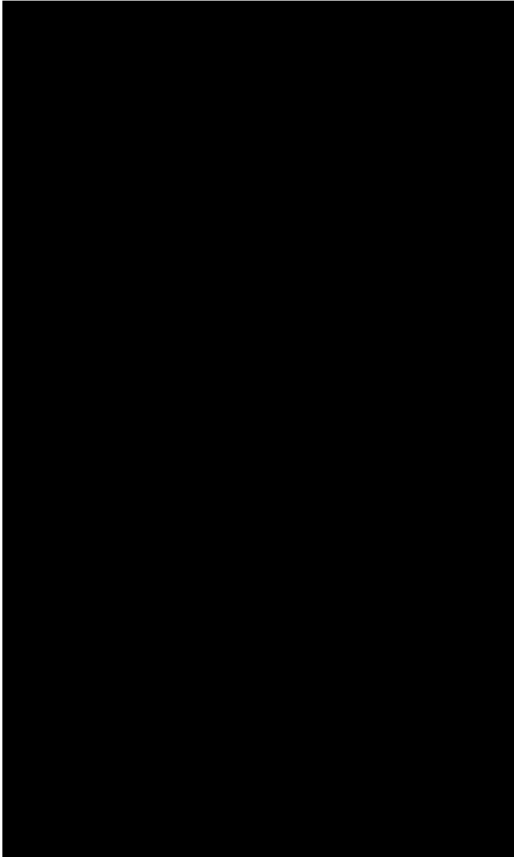
WEBSTAGRAM

# WHAT'S NEXT?



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

# SOCIAL MEDIA: TARGETED SEARCHES – SUCCESS STORY



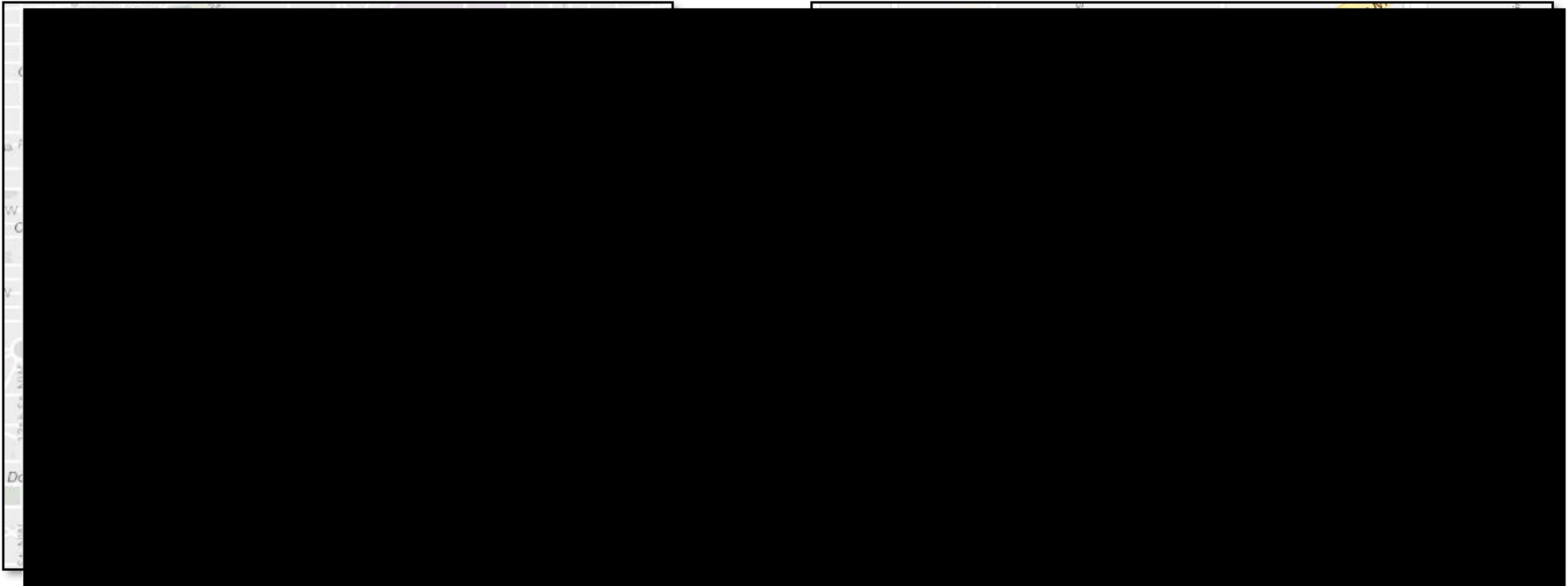


# SOCIAL MEDIA: TARGETED SEARCHES - EXAMPLE



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]

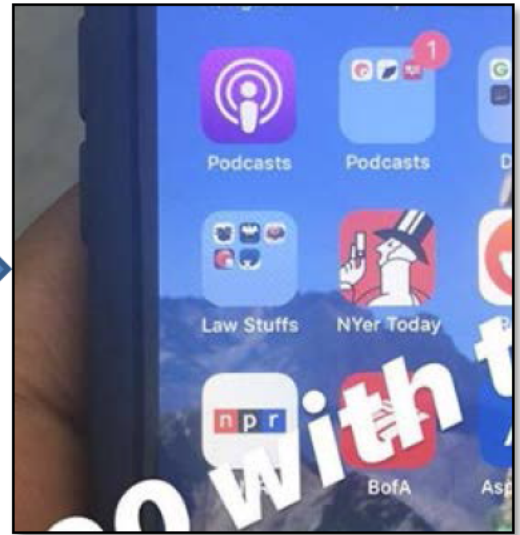
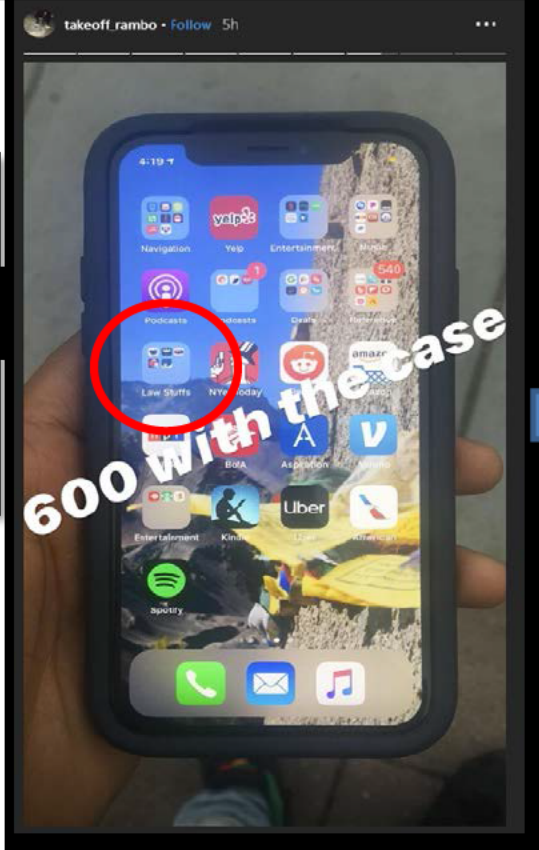
License Status: Active

[REDACTED]

County: Non-California County

[REDACTED]

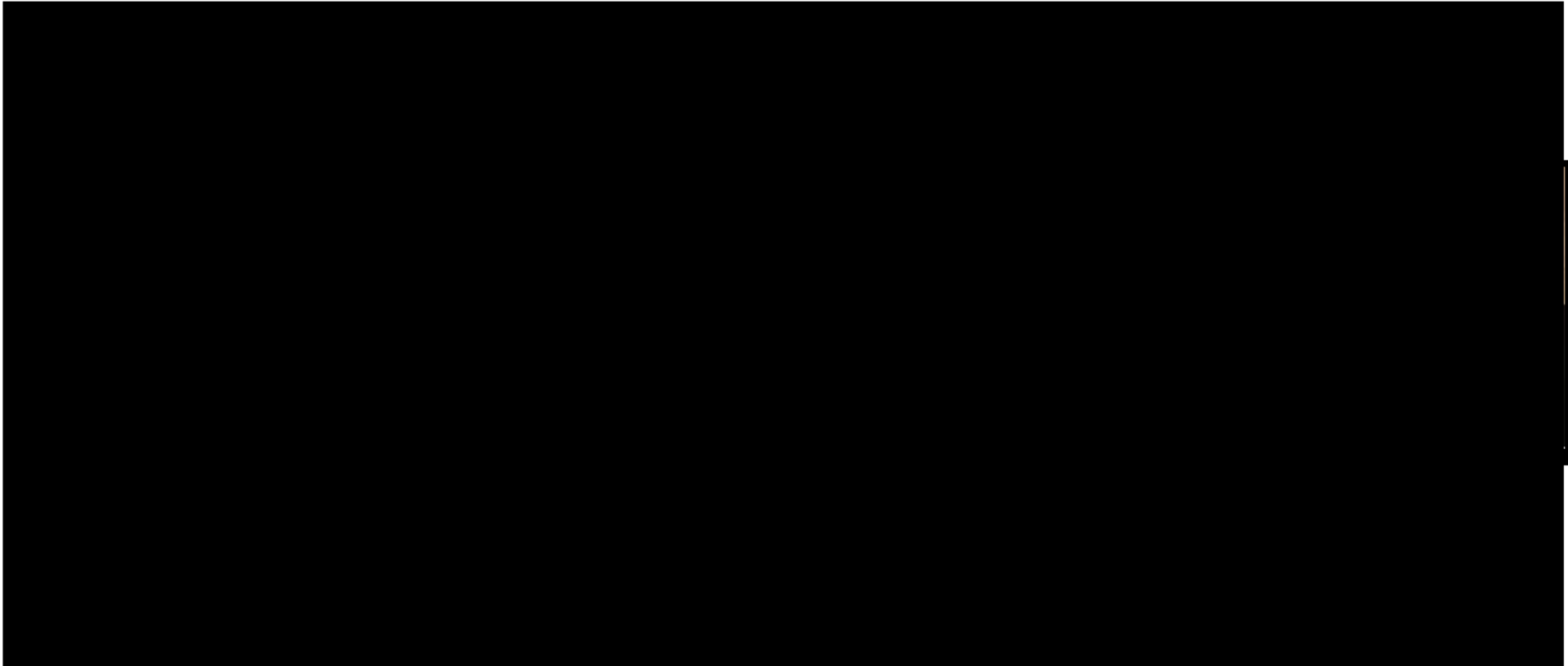
Law School: UC Berkeley SOL Boalt Hall; Berkeley CA





# 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](http://WWW.MPDC.DC.GOV)

# Exhibit G

## Totals

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