*Please Note: This is a working draft of Directive 0311.50 Investigative Use of Social Media. The PPB has not implemented any portion of this draft. Submit your comments using the "Provide Feedback Here" link located at the end of the directive.

A redline copy of the updated directive is included in this attachment.

0311.50 Investigative Use of Social Media

Second Universal Review: 6/1/23 – 07/1/23

Refer:

- ORS § 181A.250 Specific Information Not to be Collected or Maintained
- City of Portland Human Resources Administrative Rule 4.08(A) Social Media
- Directive 0310.50 Truthfulness
- Directive 0311.40 Personal Use of Social Media
- Directive 0660.00 Management of Criminal Intelligence Files

Definitions:

- Alias Social Media Account: A social media account maintained by a Bureau member under a false or fictious name, or persona.

- Criminal Intelligence: Investigative information that has been collected; analyzed and validated through police reports, field notes, records, systems, or databases to establish a link between entities and criminal activity. Intelligence includes information pertaining to the activities and associations of: 1) Individuals who, based upon reasonable suspicion, are suspected of being or having been involved in a) the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts; or b) criminal activities with known or suspected crime figures. 2) Organizations, businesses, and groups which based upon reasonable suspicion are suspected of being or having been a) involved in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts; or b) illegally operated, controlled, financed, or infiltrated by known or suspected crime figures.

- Social Media: Websites and other forms of Internet communication used to provide or share information, ideas, messages, photographs, videos and other content. Examples of social media sites include, but are not limited to, Facebook, Twitter, Instagram, YouTube, Snapchat, Reddit, Tumblr and LinkedIn. Social Media does not include sites primarily intended for commercial transactions such as ebay, or craigslist.

- Open Source Social Media: Open Source Social Media is any content for which there is no reasonable expectation of privacy as defined by the 4th Amendment of the United States Constitution, and relevant case law.

Policy:

1. The use of social media for law enforcement purposes ranging from locating missing and endangered persons, tracking threats from extremist groups, and criminal investigations is

*Please Note: This is a working draft of Directive 0311.50 Investigative Use of Social Media. The PPB has not implemented any portion of this draft. Submit your comments using the "Provide Feedback Here" link located at the end of the directive.

A redline copy of the updated directive is included in this attachment.

increasingly essential to police functioning. The Bureau recognizes that its members may need to use social media for a variety of these legitimate purposes however;

2. Law enforcement use of social media implicates core Bureau values of privacy, freedom of expression, and association. This directive seeks to establish rules that protect those values, while offering clear guidance to members about use. The Bureau expects its members to follow those rules and hold themselves to a high standard of professionalism when using social media for investigative purposes.

Procedure:

1. General Restrictions on the Investigative Use of Social Media.
   1.1. In accordance with ORS § 181A.250, members shall not collect or maintain information about the political, religious, or social views, associations or activities of any individual, group, association, organization, corporation, business or partnership unless such information directly relates to an investigation of criminal activities, and there are reasonable grounds to suspect the subject of the information is or may be involved in criminal conduct.

   1.2. Criminal intelligence is distinct from information gathered for a specific investigation Specific information gathered from social media as part of an investigation is not criminal intelligence unless it has been analyzed, validated, and is part of a broader profile of a person engaged in criminal activity or a criminal enterprise. Criminal intelligence gathered from social media must be gathered and maintained in accordance with Directive 0660.00, Management of Criminal Intelligence Files.

   1.3. Members may not use personal devices or personal accounts for investigative purposes.

   1.4. Members may only use deception on social media in accordance with the restrictions set forth in this directive, and directive 0310.50 Truthfulness.

2. Open-Source Social Media Investigations.
   2.1. Members may access open-source social media for any valid law enforcement purpose.

   2.2. Any information retained, (e.g. transcribed, screen shotted, or recorded) from a social media source should be documented in accordance with Section 5. of this directive.

3. Alias Accounts.
   3.1 Members may maintain an alias social media account, either individually or collectively with other members for law enforcement purposes, either
      3.1.1 When the alias account and its purpose has been approved by the member's supervisor; or in accordance with a unit SOP that outlines the valid uses of social media for that unit.

*Please Note: This is a working draft of Directive 0311.50 Investigative Use of Social Media. The PPB has not implemented any portion of this draft. Submit your comments using the "Provide Feedback Here" link located at the end of the directive.

A redline copy of the updated directive is included in this attachment.

3.2. All Alias Accounts are subject to supervisory review.
3.2.1. Supervisors may review a member's Alias Account at any time.
3.2.2. Supervisors shall include their subordinate's investigative use of social media as part of their regular performance reviews.

4. Alias Account Communication.
4.1. Members may use Alias Accounts to communicate with persons when one of the following conditions is met:
4.1.1. There is reasonable suspicion to believe a crime has been committed or is going to be committed;
4.1.2. There is a specific threat to an individual or the public;
4.1.3. To maintain the alias established by the account, for example when contacted by another party.
4.1.4. Any other use of an alias account must receive specific approval from a supervisor.

4.2. For the purposes of this directive, "communicate" means only narrative communication with a specific individual or individuals such as a direct message. It does not include "liking," "sharing," posting curated content, or their equivalents.

4.3. Units that expect members to maintain alias social media accounts, must develop SOPs governing the use of communications through alias accounts.

5. Documentation:
5.1. Any information obtained or retained (e.g. transcribed, screenshotted or recorded) from social media should be documented in an appropriate police report, case file, or in accordance with a unit SOP. If the information gathered is not part of a specific ongoing investigation the documentation should include a brief description of the law enforcement purpose for the capture.
5.2. No communication through an alias account may be deleted or destroyed.
5.3. Any communication through an alias account that is not covered by a unit SOP must be saved as a transcription, screen shot or photo.

6. Refer to Directive 0311.40, Personal Use of Social Media for rules governing personal use of Social Media.

Provide Feedback Here

0311.50 Investigative Use of Social Media

Refer:

- ORS § 181A.250 Specific Information Not to be Collected or Maintained
- City of Portland Human Resources Administrative Rule 4.08(A) Social Media
- Directive 0310.50 Truthfulness
- Directive 0311.40 Personal Use of Social Media
- Directive 0660.00 Management of Criminal Intelligence Files

Definitions:

- Alias Social Media Account: A social media account maintained by a Bureau member under a false or fictious name, or persona.

- Criminal Intelligence: Investigative information that has been collected; analyzed and validated through police reports, field notes, records, systems, or databases to establish a link between entities and criminal activity. Intelligence includes information pertaining to the activities and associations of: 1) Individuals who, based upon reasonable suspicion, are suspected of being or having been involved in a) the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts; or b) criminal activities with known or suspected crime figures. 2) Organizations, businesses, and groups which based upon reasonable suspicion are suspected of being or having been a) involved in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts; or b) illegally operated, controlled, financed, or infiltrated by known or suspected crime figures.

- Social Media: Websites and other forms of Internet communication used to provide or share information, ideas, messages, photographs, videos and other content. Examples of social media sites include, but are not limited to, Facebook, Twitter, Instagram, YouTube, Snapchat, Reddit, Tumblr and LinkedIn. Social Media does not include sites primarily intended for commercial transactions such as ebay, or craigslist.

- Open Source Social Media ~~Search: A~~: Open Source Social Media ~~search~~ is any ~~check or browsing of a social media site looking~~content for ~~information. This could include looking for a specific account, or specific information using a search engine, or checking a particular account. A "Social Media Search"~~which there is ~~not inherently a search for 4th Amendment purposes, and members must evaluate whether any given use of Social Media implicates~~no reasonable expectation of privacy as defined by the 4th Amendment ~~based on~~of the ~~totality of the circumstances and current~~United States Constitution, and relevant case law.

Policy:

1. ~~Social media can be an essential investigative tool, providing members with key evidence in criminal investigations.~~The use of social media for law enforcement purposes ranging from locating missing and endangered ~~people~~persons, tracking threats from extremist groups, and ~~safely resolving dangerous incidents. However, the use of social media also~~ criminal

investigations is increasingly essential to police functioning. The Bureau recognizes that its members may need to use social media for a variety of these legitimate purposes however;

~~1.~~2. Law enforcement use of social media implicates core Bureau values of privacy, freedom of expression, and association. ~~As such the~~This directive seeks to establish rules that protect those values, while offering clear guidance to members about use. The Bureau expects its members to ~~use social media judiciously~~follow those rules and ~~in accordance with the procedures laid out in this directive~~hold themselves to a high standard of professionalism when using social media for investigative purposes.

Procedure:

1. General Restrictions on the Investigative Use of Social Media.

1.1. In accordance with ORS § 181A.250, members shall not collect or maintain information about the political, religious, or social views, associations or activities of any individual, group, association, organization, corporation, business or partnership unless such information directly relates to an investigation of criminal activities, and there are reasonable grounds to suspect the subject of the information is or may be involved in criminal conduct.

1.2. Criminal intelligence is distinct from information gathered for a specific investigation Specific information gathered from social media as part of an investigation is not criminal intelligence unless it has been analyzed, validated, and is part of a broader profile of a person engaged in criminal activity or a criminal enterprise. Criminal intelligence gathered from social media must be gathered and maintained in accordance with Directive 0660.00, Management of Criminal Intelligence Files.

1.3. Members may not use personal devices or personal accounts for investigative purposes.

~~1.3.~~1.4. Members may only use deception on social media ~~for investigative purposes while on duty~~in accordance with the restrictions set forth in this directive, and ~~using Bureau issued electronic devices~~directive 0310.50 Truthfulness.

2. Open-Source Social Media Investigations.

~~1.4.~~2.1. Members may access ~~publicly available information on~~open-source social media~~, (e.g. viewing a public profile),~~ for ~~a~~any valid law enforcement purpose ~~including, but not limited to the following:~~ .

~~1.4.1. Any Conducting a criminal investigation.~~
~~1.4.2. Locating a wanted, missing, or potentially suicidal person.~~
~~1.4.3. Aiding the coordination of police resources.~~
~~1.4.4. Conducting a pre-employment background check, or conducting an administrative investigation.~~

2.2. information retained, (e.g. transcribed, screen shotted, or recorded) from a social media source should be documented in accordance with Section 5. of this directive.

~~2.~~3. Alias Accounts.

3.1 Members may maintain an alias social media account~~-~~, either individually or collectively with other members for ~~investigative~~ law enforcement purposes ~~under the following conditions:~~, either

3.1.1 ~~The~~When the alias account and its purpose has been approved by the member's supervisor; or in accordance with a unit SOP that outlines the valid uses of social media for that unit.

~~2.1.1.1. The account, including username and password, has been registered with the Bureau.~~

3.2. All Alias Accounts are subject to supervisory review.

3.2.1. Supervisors may review a member's Alias Account at any time.

3.2.2. Supervisors shall include their subordinate's investigative use of social media as part of their regular performance reviews.

4. Alias Account Communication.

~~2.2.~~4.1. Members may use Alias Accounts to ~~interact~~communicate with persons when one of the following conditions is met:

~~2.2.1.~~4.1.1. There is reasonable suspicion to believe a crime has been committed or is going to be committed~~.~~;

4.1.2. There is a specific threat to an individual or the public;

4.1.3. To maintain the alias established by the account, for example when contacted by another party.

4.1.4. Any other use of an alias account must receive specific approval from a supervisor.

~~2.2.1.1.~~ For ~~The use has been noted in the appropriate report.~~

~~2.2.2. When posting content, members shall act in accordance with the standards set forth in Directive 0310.50, Truthfulness.~~

4.2. the purposes of this directive, "communicate" means only narrative communication with a specific individual or individuals such as a direct message. It does not include "liking," "sharing," posting curated content, or their equivalents.

4.3. Units that expect members to maintain alias social media accounts, must develop SOPs governing the use of communications through alias accounts.

~~3.~~5.Documentation:

Any ~~search of~~ information obtained or retained (e.g. transcribed, screenshotted or recorded) from social media ~~for an investigative purpose must be documented. This documentation must include the case number of the investigation, the purpose, and general scope e.g. social media sites checked.~~

~~3.1.1.1. For~~ ~~members making only occasional, case specific investigative use of social media, the documentation~~ should be ~~made~~documented in an appropriate police report, case file, or ~~as notes~~ in ~~the relevant CAD call.~~

~~For investigators who use social media as part of ongoing, complex investigations and intelligence gathering, they should maintain a log listing the above information.~~ accordance with a unit SOP. If the

~~3.2.~~5.1. ~~Any~~ information gathered ~~from~~is not part of a specific ongoing investigation the ~~investigative use of Social Media~~documentation should ~~be specifically noted in~~include a brief description of the ~~appropriate police report, with~~law enforcement purpose for the ~~source listed~~capture.

~~3.2.1. Any posts made to an Alias Account shall be transcribed into an appropriate police report, criminal intelligence file system, or as a screenshot uploaded into the DIMS photo management system.~~

5.2. No communication through an alias account may be deleted or destroyed.

5.3. Any communication through an alias account that is not covered by a unit SOP must be saved as a transcription, screen shot or photo.

~~4.~~6. Refer to Directive 0311.40, Personal Use of Social Media for rules governing personal use of Social Media.

#1

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Tuesday, February 28, 2023 4:34:48 PM
Last Modified: Tuesday, February 28, 2023 4:34:57 PM
Time Spent: 00:00:08

Page 1

Q1

Please provide feedback for this directive

test

Q2

Respondent skipped this question

Contact Information (optional - your name will be visible on PPB's website)

#2

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Wednesday, March 01, 2023 2:58:07 PM
Last Modified: Wednesday, March 01, 2023 3:02:06 PM
Time Spent: 00:03:59

Page 1

Q1

Please provide feedback for this directive

As an investigator, open-source information is imperative to my job. Furthermore, documenting usage of such platforms in police reports will impede new investigations, as the subjects being investigated will modify their current behavior and remove this infomation. The information gathered through these open-source platforms is invaluable in solving violent crimes in the city of Portland. The directive will further hinder investigations in the city of Portland

Q2

Respondent skipped this question

Contact Information (optional - your name will be visible on PPB's website)

#3

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Wednesday, March 01, 2023 3:12:02 PM
Last Modified: Wednesday, March 01, 2023 3:19:58 PM
Time Spent: 00:07:56

Page 1

Q1

Please provide feedback for this directive

Really the first draft. Might in the future, in a future case(some more clarity), a social media search is not inherently a 4th Amendment issue or needs to be used. But, in the last half, there is some uncertainty about the totality of the case, Basically, if it will be a "fruit of the poisonous tree" issue or not. Pls note, not a lawyer at all. Second, does this social media search includes all the likes or repost(share) to the social media post in question?

Q2

Contact Information (optional - your name will be visible on PPB's website)

Name	**Robbie (he or him)**

#4

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Wednesday, March 01, 2023 3:32:23 PM
Last Modified: Wednesday, March 01, 2023 3:45:26 PM
Time Spent: 00:13:02

Page 1

Q1

Please provide feedback for this directive

I have never commented on one of these. But I feel I have to on this one. It is utterly *Baffling* to me how someone could dream up such a restrictive and overburdening policy. There is plenty of long-standing documented case law on there being NO expectation of privacy on material posted on the internet by someone. Examples of such case law can be found with a simple search. Today's social media is a modern town hall to give people a medium to voice opinion and interact. Having to document each search in a manner as described will do nothing other than to slow down or stop all together the use of social media for investigative purposes. Let's do ourselves a favor stop *overthinking* this issue to the nth degree. I am curious what the logic was on this? I suspect it was made by someone with little or no investigative experience.
Stop this trainwreck before it is enacted.

Q2

Respondent skipped this question

Contact Information (optional - your name will be visible on PPB's website)

#5

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Thursday, March 02, 2023 9:26:40 AM
Last Modified: Thursday, March 02, 2023 9:36:44 AM
Time Spent: 00:10:03

Page 1

Q1

Please provide feedback for this directive

Social media can be a essential tool that can help provide evidence in cases from assaults, shootings, homicide, human trafficking, among many other cases. In those instances, investigators will already be documenting the information in accounts. To make them write a report for each time they log into their account to check on a suspect account will tie up valuable time when they need to focus that time on other aspects of the case. Secondly, having to record what the account with the bureau will potentially be subject to public disclosure and could be disseminated to the subjects that are under investigation. Therefore, this policy places restrictions that may hinder investigators.

Q2

Respondent skipped this question

Contact Information (optional - your name will be visible on PPB's website)

#6

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Thursday, March 02, 2023 10:16:43 AM
Last Modified: Thursday, March 02, 2023 10:19:57 AM
Time Spent: 00:03:13

Page 1

Q1

Please provide feedback for this directive

0311.50 Investigative Use of Social Media

Q2

Respondent skipped this question

Contact Information (optional - your name will be visible on PPB's website)

#7

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Thursday, March 02, 2023 10:20:09 AM
Last Modified: Thursday, March 02, 2023 11:09:38 AM
Time Spent: 00:49:28

Page 1

Q1

Please provide feedback for this directive

0311.50 Investigative Use of Social Media

"Members may only use social media for investigative purposes while on duty..."

This is unclear to me. Does "on duty" mean when working as part of one's regular shift or on documented overtime? If this is the case I believe that it hinders investigations and is out of touch with the complex nature of investigations.

Social media is so common now that most individuals make use of it. Individuals use of social media can be incredibly valuable to investigations as it can establish patterns of life, associations with others involved in the investigation, travel, physical descriptors, etc etc. Social media account postings can be ephemeral. Postings on Instagram and Snapchat for example may only last for 24 hours and in many instances the postings are deleted before then. Investigators, either officers or detectives, most commonly work a day shift (0700-1700). However, it is not uncommon for individuals that are subject to investigations to be active outside of these hours. The ability of an investigator to search (policy definition) a social media account outside traditional hours of work is essential to investigations. This outside "work" work is not abnormal for investigators and is indicative of hard-working employees who care about their work. It does not imply anything out of policy or shady is occurring. The "search" is still being conducted on a bureau issued electronic device and subject to the same policy rules but does not unintentionally hinder an investigators capability.

"Alias Accounts: The account, including username and password, has been registered with the Bureau."

I am concerned about this because I feel like it would be subject to public records requests. While transparency in law enforcement is important, it is also essential for law enforcement to have tools and investigative abilities. Alias social media accounts can take years to obtain legitimacy and be of optimal use. If investigators alias accounts are released as part of public records requests they will immediately be of no use. Not only that, it would likely inform a subject of a criminal investigation that law enforcement was interested in them. This would greatly hinder and investigation.

"Documentation: Any search of social media for an investigative purpose must be documented."

This would be a great burden for investigators. I access social media for investigative purposes, sometimes, dozens of times during my shift for various reasons including locating victims of crimes, locating suspects of crimes, for ongoing investigations, etc. These "searches" are not necessarily linked and can be for different reasons or cases. Therefore, in addition to all the documentation requirements already required of investigators, the difficulties and demands of being engaged in complex investigations, it would then be required to potentially write a dozen additional reports each shift just for social media access. These social media "Searches" are often preliminary and may not always result in an investigation. Therefore, an investigator would have to obtain a case number, create a General Offense report, add entities, write a narrative, etc for each instance. This may not seem like a big deal for someone unfamiliar to our documentation process. I can say conservatively, on average, that each one of these social media documentations would take 15 minutes. If, like stated before, I "search" social media a dozen times a shift, that could potentially be three hours of documentation. That may sound like hyperbole but in my job the use of social media under this policy could require that.

I believe the policy should be general in nature and direct officers/investigators to use alias social media accounts professionally and within the confines of the law and other policies. I believe supervisor notification that an investigator uses an alias account is appropriate. The micromanaging of officer's use of tools and techniques, specifically in ways outlined above, is a hinderance to criminal investigation and the motivation of investigators.

Q2

Contact Information (optional - your name will be visible on PPB's website)

Respondent skipped this question

#8

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Friday, March 03, 2023 2:32:07 PM
Last Modified: Friday, March 03, 2023 2:42:53 PM
Time Spent: 00:10:46

Page 1

Q1

Please provide feedback for this directive

This policy is overly restrictive and at points completely unnecessary. Why would you want to reveal an alias account in a police report that is then discoverable and hence compromises the alias account? Also creating a log is unnecessary and unneeded redundancy. If an item of evidence is discovered via social media and it is found via public viewably format not a search warrant then it is public domain. The reference and information will obviously be documented and how it was obtained will be listed. If the social media evidence is obtained through a search warrant then this to will document how the and where it was obtained. This policy creates unnecessary work and exposes investigative tools and processes in such a way to that will limit and compromise future investigations. There is no legal or best practice format to justify these limitations. You are inhibiting your investigators and will only allow subjects to continue their criminal conduct by implementing such a policy.

Q2

Respondent skipped this question

Contact Information (optional - your name will be visible on PPB's website)

#9

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Monday, March 06, 2023 10:24:42 AM
Last Modified: Monday, March 06, 2023 11:07:34 AM
Time Spent: 00:42:51

Page 1

Q1

Please provide feedback for this directive

1.5.1.2- This provision takes control of an account out of the hands of an investigator and could expose members to unauthorized logins if account information is registered with the "Bureau".

1.5.3- the requirement for "truthfulness" contradicts the very nature of undecover/covert investigations. i.e does an investigator communicating or posting with a child pedophile suspect have to be "truthful" with the suspect? And if they were deceptive, subject to violation of this provision?

1.6.1-"Any search" is too broad. many sites/profiles often are irrelevant or unrelated to the investigation and requiring they be listed is unnecessary. Also often times, particular profiles are of confidential informants or people who want to provide information, but who aren't willing to be named as a source out of fear or retaliation. Requiring their profile to be documented could expose them to physical risk.

1.6.1.1- Again unnecessary. Entering notes in a CAD call could again run afoul for the reasons stated above.

1.6.3.- Again unnecessary.

This directive is drafted seemingly as a solution seeking a problem. Investigators already document in reports, affidavits and subsequent discovery material, critical case information that helps build a case that was derived from social media outlets. The added requirements of documentation, for the sake of documentation, as noted above will only serve to give pause to cooperating individuals, curtail investigations or worse, expose cooperating witnesses and persons to life safety issues.

Before continuing with this policy, I would highly recommend speaking with a panel of experienced investigators about the intended or unintended implications, and the intended or unintended consequences, of this proposed directive. The policy writer(s) owe it to those doing the important work of conducting serious investigations.

Q2 **Respondent skipped this question**

Contact Information (optional - your name will be visible on PPB's website)

#10

COMPLETE

Collector: Web Link 1 (Web Link)
Started: Thursday, March 09, 2023 2:59:33 PM
Last Modified: Thursday, March 09, 2023 3:04:04 PM
Time Spent: 00:04:30

Page 1

Q1

Please provide feedback for this directive

This directive is incredibly clunky. There is no need to document every single search or link via social media that is open source, as it is open source. That is a huge time suck and you may not know how or where a connection may go on the front end. Once there is PC for an account, warrants are obtained and served.

What type of "log" should be used and how would things be documented and maintained? Registering an account with the bureau is also pointless. Who approves it, what shall that look like? Many investigators have accounts they have used for years to look at open source social media. This policy is more restrictive than law and ridiculous.

Q2

Respondent skipped this question

Contact Information (optional - your name will be visible on PPB's website)

#11

COMPLETE

Collector:	Web Link 1 (Web Link)
Started:	Thursday, March 30, 2023 11:18:38 AM
Last Modified:	Thursday, March 30, 2023 1:01:11 PM
Time Spent:	01:42:32

Page 1

Q1

Please provide feedback for this directive

-IACP Law Enforcement Policy Center (article is Social Media: Considerations, May 2019) has a better articulation of definitions for social media, social network. The current definition should be more broad and provides no clarification that each platform has a different layout, format, search process, communication format, messaging options, etc
-Currently at the federal level, there is no specific legislative framework or federal laws that governs law enforcement use of information obtained social media. It should be noted this directive is more restrictive.
-The public end user has the ability to accept/deny any requests that are sent to their account from an alias account. It is their choice and ability to further investigate the alias account. They possess the control to allow the alias account to gain access. There is no coercion occurring for the acceptance.
-This policy documents investigative purposes, but what about social media accounts that represent the Bureau in some fashion (the ppb main account, ppb bike central account, the chief's accounts, precinct accounts, etc). Is there a corresponding policy that has same/similar restrictions. The level of monitoring and documentation is significantly different, with those being direct representations of the Bureau and its professionalism.
-Responding to Procedure 1.1 - while the intent is understood for the meaning of this language, it is written in a fashion that directly conflicts with information/intel that was collected during civil unrest. Some of the groups (representing all sides) have specific affiliations and the direct monitoring of those, publicly or with alias accounts, is critical for the safety of the community. While not all information elevates to that level, if resources need to be planned related to planned criminal activity, prohibiting the monitoring of self-proclaimed politically or socially driven groups is inappropriate.
-Responding to Procedure 1.3 - ...bureau "issued" electronic devices... should be changed to ...bureau "approved"... Devices that are not networked for investigative purposes are approved by someone, but not necessarily issued to a particular person.
-Responding to Procedure 1.4.3 - Is this content to include alias accounts used to contact victims of a crime to when no other means have been effective?
-Responding to Procedure 1.5.1.2 - who maintains this information, where is it stored, who updates it? Is this subject to public records request - if so that could significantly compromise a victim's safety or investigation.
-Responding to Procedure 1.5.3 - The truthfulness directive could contradict the ORS that allows officers to lie (not to juveniles) for purposes of an investigation. The directive that might be more appropriate would be related to professionalism to ensure people are not posting content or acting in a manner that would be offensive.
-Responding to Documentation 1.6.1 - to document every search is excessive and inappropriate amount of wasted time for officers. A search could include following links to identify "friends" or other pages that are relevant to an investigation.
-Responding to Documentation 1.6.1.2 - Does the log become part of a report? Does the log replace documenting every time or is it inclusive and only one documentation at the end of the investigation suffice?
-Responding to Documentation 1.6.2 - Any information that is gathered that is relevant to an investigation is often preserved/legally obtained from the social media source through legal means to corroborate what was located. This directive gives no credit to information that is legally obtained in a rightful manner, following the investigative searches using an alias account.
-Responding to Directive 1.6.3 - If a supervisor has provided approval for the account and abiding by all other required policies, and if documentation is needed in a report, the screen shot of the same is unnecessary duplication. Also, what if there is no case number generated yet? It is simply information that is being viewed and has not been fully converted into intelligence. This could be viewed from a community policing standpoint as some cases are made from content that was observed online (guns, drugs, compelling prostitution, accomplice in a crime, etc.)
-What if I look up a user's account name and information for the sole purpose of the other investigator requesting a legal process? Do I now have to document the same when it is documented in the legal process?
-The directive does not expressly mention urgent events affecting the community/life safety of many (ie. bombing, mass shooting, etc) where LEO has the ability to contact social media directly for assistance in a law enforcement manner
-There is no clarification regarding content viewed through an alias account that is actually open source information viewable to any member of the public.
-What if multiple users in the same unit utilize/access information from the same alias account? With the level of documentation currently required it would create an unclear picture regarding the use.
-As it relates to content viewed, perhaps note that information acquired from social media will be evaluated to assess reliability and

validity and legal process will be completed if deemed investigatory
-Currently the Delaware Supreme Court has upheld that a multi-year monitoring of a social media account did not violate the 4th amendment. I assume the 9th district has no corresponding case at this current time. This directive would significantly impact long term investigations and the amount of documentation for viewing content in a monitoring manner. Each person can freely post as they choose and therefore an investigation should not be hindered due to that. Social media has essentially become speaking freely in a 'public' place, but in a virtual format. For those wishing their content and information be allowed to be viewed, they are expressing themselves freely. Each user can significantly limit the amount of content other viewers can see.
-The easiest way to summarize the specifics and allow for appropriate interpretation and modifications in the future is to say "this policy states that the use of social media to access information for criminal investigations must comply with applicable laws and policies regarding privacy, civil rights, and civil liberties.
-Also, please make this comment box much larger!!! The selecting of text is highly sensitive and is not user friendly in allowing the commenter to review their information for correctness. So, please forgive any typos or grammatical errors.

Q2

Respondent skipped this question

Contact Information (optional - your name will be visible on PPB's website)