

Table of Contents

I.	Back	Background		
		Criminal Intelligence Unit	1	
II.	Inve	stigation Methodology	3	
III.	Findings			
IV.	Witness Interviews and Observations			
	1.	—Research Analyst 3	7	
	2.	—Research Analyst 3	8	
	3.	—Research Analyst 3	9	
	4.	—Research Analyst 3	11	
	5.	—Special Agent	12	
	6.	—Special Agent	17	
	7.	David Kirby—Special Agent in Charge	18	
	8.	Darin Tweedt—DOJ Chief Counsel	20	
	9.	—Research Analyst 4	23	
	10.	Steven McIntosh—Assistant Special Agent in Charge of CJD	24	
	11.	Matt McCauley—Assistant Attorney General	26	
V.	Cone	clusions and Recommendations	28	

I. Background

On November 4, 2015, I was contacted by Lisa Umscheid, an attorney with the Oregon Department of Justice ("DOJ"), regarding my availability to conduct an investigation into the use of a digital monitoring software platform by at least one employee of the DOJ's Criminal Justice Division ("CJD" or "division"). By contract effective November 10, 2015, the DOJ retained me under the supervision of the DOJ's Supervising Attorney, Ms.Umscheid, to (a) conduct an investigation into any improper conduct and performance of employees with regard to their compilation, analysis, monitoring and use of digital information (such as content posted on websites, social media or Twitter feeds) in the course of any work performed as employees of DOJ; and (b) advise DOJ regarding the scope of an audit of the CJD's compilation, analysis, monitoring and use of digital information in connection with the division's work.

This investigation was initiated by order of Oregon Attorney General Ellen Rosenblum after she learned that DOJ/CJD employee, used social media monitoring software that was being tested for potential purchase by the DOJ to conduct a search using search terms including #blacklivesmatter. The search resulted in a review of the Twitter account of Erious Johnson, Jr., Director of Civil Rights for DOJ and Office of Attorney General, and generated a report on the outcome of the search. The Attorney General notified Mr. Johnson of this report, subsequently called for this investigation into the matter and placed on administrative leave pending the outcome of the investigation.

is an investigator assigned to the Oregon TITAN Fusion Center, which is a unit within the CJD's Criminal Intelligence Unit. An overview of the Criminal Intelligence Unit, as provided in writing by former DOJ Chief Counsel Darin Tweedt, is set forth below:

Criminal Intelligence Unit

The ability to gather and analyze information about criminals and their organizations is invaluable to law enforcement agencies. The Criminal Intelligence Unit, aka

(continued . . .)

¹ The benefits of gathering and analyzing criminal information was recognized by the Oregon legislature in 1977 when it directed the Department of Justice to:

⁽²⁾ Establish a coordinated system of collecting, storing and disseminating information relating to organized crime.

⁽³⁾ Develop and maintain a liaison between local, state and federal law enforcement agencies in Oregon, assisting them in the investigation and suppression of organized criminal activity and encouraging cooperation among those agencies.

⁽⁴⁾ Conduct comprehensive factual studies of organized criminal activity in Oregon, outlining existing state

and local policies and procedures with respect to organized crime, and formulating and proposing such changes in those policies and procedures as the department may deem appropriate.

Criminal Intelligence Center, facilitates the gathering, analysis and sharing of criminal information with local, state and national law enforcement agencies. The Unit is composed of the Oregon TITAN Fusion Center, the Oregon HIDTA Investigation Support Center, and the Oregon HIDTA Watch Center.

• <u>Oregon TITAN Fusion Center</u>: The Fusion Center is Oregon's focal point for receiving, analyzing, gathering, and sharing threat-related information in order to better detect, prevent, investigate, and respond to criminal and terrorist activity.

The Fusion Center is composed primarily of staff from the Criminal Justice Division.² This staff works in conjunction with federal, state and local law enforcement agencies. The Fusion Center produces threat assessments³, officer safety bulletins, general crime bulletins and terrorism related bulletins. In addition, the Fusion Center is an essential component of the state's critical infrastructure review process. The Fusion Center also provides criminal analysts to assist federal, state and local law enforcement agencies with criminal investigations. Finally, the Center provides important training to law enforcement agencies, businesses and first responders about active shooters and the latest terrorist trends, techniques and procedures.

• <u>High Intensity Drug Trafficking Area (HIDTA) Investigation Support</u>

<u>Center:</u> The Investigation Support Center is a co-located multi-agency program. Its mission is to promote, facilitate, and coordinate the exchange of criminal intelligence information, and provide analytical support. The Criminal Justice Division has five Research Analysts assigned to the Investigation Support Center.

(... continued) ORS §180.610 (2), (3) (4).

Oregon TITAN Fusion Center Procedure, Threat Assessments/Risk & Vulnerability Assessments, September 18, 2015.

² The Criminal Justice Division component is one attorney, one Special Agent, five Research Analysts and an IS Specialist.

³ A threat assessment is the "[p]rocess of identifying or evaluating entities or events for indications of potential harm to life, property, operations or information. These assessments involve investigative research which results in a written product identifying possible threats to a specific person or incident. Examples include Pendleton Round-up, Hillsboro Air Show or Governor's Inauguration. Threat assessments may be conducted by an individual or team of analysts based on the complexity of the assessment."

• <u>High Intensity Drug Trafficking Area (HIDTA) Watch Center</u>: The Watch Center's primary mission is to enhance officer safety through deconfliction for the designated HIDTA counties. Watch Center analysts also provide tactical analytical support to law enforcement officers throughout Oregon. The Criminal Justice Division has three Research Analysts and a supervisor assigned to the Investigation Support Center.

See Ex. A (November 25, 2015 Memorandum from Darin Tweedt).

II. Investigation Methodology

Prior to conducting witness interviews, I met with various DOJ employees to obtain background information on the CJD and the circumstances that led to the decision to conduct the investigation that is the subject of this report. These individuals included: DOJ Senior Assistant Attorney General Lisa Umscheid, Deputy Attorney General Fred Boss and DOJ Special Counsel on Public Safety Michael Slauson.⁵

Beginning December 15, 2015, I conducted face-to-face interviews with CJD employees and obtained background information and documents relevant to the Attorney General's concerns. At the start of each interview, I explained my role as an investigator hired by DOJ to conduct an investigation into the facts and provide recommendations to DOJ. I explained that the statements made by the witnesses would be shared with the DOJ, but that the witnesses should not discuss our interview with others. I also explained the Garrity rights notices that were provided to the witnesses.

I reminded these employee witnesses that there could be no retaliation either by or against them for anyone's participation in the investigation, and to immediately notify HR if they experienced retaliation. I provided the witnesses with my business card and invited them to contact me if they had any other information or documentation to share.

⁴ Deconfliction is a process designed to ensure that multiple agencies are not inadvertently targeting the same event, individual, or organization. Deconfliction occurs when officers of one investigative agency are notified that officers of another agency may be conducting operations in the same area or may be investigating the same suspect. Deconfliction prevents costly duplication of investigative effort and compromise of investigations. Most importantly, deconfliction directly impacts officer safety by reducing the chances two law enforcement agencies, unbeknown to each other, are carrying out undercover law enforcement operations in the same area.

⁵ Mr. Slauson has since assumed the position of Acting Chief Counsel of the CJD.

⁶ Note, I have been informed that under the terms of their collective bargaining agreement, union employees are permitted to engage in discussions with others regarding the investigation.

To better understand the search methodology used by and others, I requested training on the software that was used for the search. The company that developed and owns the software ("Digital Stakeout") that was used for the search cooperated with DOJ's request to provide me with an abbreviated general overview demonstration/training on the software.

I further requested that the DOJ conduct a thorough search of CJD computers used by to determine the scope of his searching and activity regarding #blacklivesmatter and other relevant search terms.

As part of my investigation, I requested a copy of all CJD policies, procedures or protocols relevant to privacy rights of individuals and groups and how and when information could be gathered. I received and reviewed the following division policies:

- o Oregon TITAN Fusion Center Privacy Policy. See Ex. B.
- o Social Media Non-Covert Investigation Policy 3-101.5 dated July 31, 2015. See Ex. C.
- o Fusion Center Procedure for Threat Assessments dated September 18, 2015. See Ex. D.
- o Oregon TITAN/Fusion Center Policy Regarding First Amendment Protected Events. See Ex. E.

I also reviewed the following statutes and regulations relevant to CJD employees:

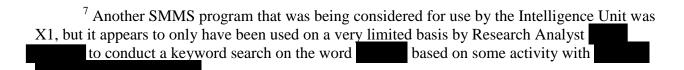
- 28 CFR Part 23 regarding Criminal Intelligence Systems Operating Policies. This federal regulation applies to state agencies if they are operating inter- or multi-jurisdictional criminal intelligence systems that are supported with Crime Control Act funding. The regulation forbids the collection or maintaining of criminal intelligence information about the political, religious or social views, associations or activities of any individual or any group, association, corporation, business, partnership or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity. See 28 CFR §23.20(b).
- ORS §181.575 (now recodified as ORS §181A.250) states that "no law enforcement agency, as defined in ORS §181.010 (Definitions for ORS §\$181.010 to 181.560 and 181.715 to 181.730), may 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."

My findings, summary of the interviews and observations, conclusions and recommendations are below.

III. Findings

1. In early 2015, Chief Counsel Darin Tweedt directed Special Agent In Charge Steve McIntosh to identify and test social media monitoring software ("SMMS") programs that could be helpful in criminal investigations supported or conducted by the CJD.

- 2. On September 29, 2015, certain CJD employees within the Intelligence Unit were given a demo and some training by the vendor of an SMMS product, Digital Stakeout. Digital Stakeout takes user specified keywords and searches multiple open source social media sites, and returns results that can be pinpointed to a geographic area specified by the user. The vendor allowed the employees to use Digital Stakeout on a free trial basis after the demo, and some employees tested it for a period of time. ⁷
- 3. On September 30, 2015, Agent used Digital Stakeout to conduct a search on the keyword search term "#blacklivesmatter" combined with "#fuckthepolice" ("the search"). He focused his search on Salem, Oregon, which yielded results that included Twitter posts by Erious Johnson, Jr. believed that some of Mr. Johnson's posts were threatening to the police and he verbally shared his concerns with Special Agent in Charge David Kirby.
- 4. Mr. Kirby verbally described the concerning posts to Mr. Tweedt, and based on the description, Mr. Tweedt recommended to Deputy Attorney General Fred Boss that prepare a report on his search and the findings. Mr. Boss approved this recommendation and was then directed to write the report.
- 5. On October 1, 2015, prepared and presented to Mr. Kirby a report he referenced as "Possible threats towards law enforcement by DOJ employee." This report was a single page memo with an attachment that included several pages of posts that printed directly from Mr. Johnson's Twitter feed rather than from Digital Stakeout. See Ex. F.
- 6. On October 8, 2015, Mr. Kirby delivered the report to Deputy Chief Counsel Stephanie Tuttle. In an email to Mr. Tweedt, Mr. Kirby reiterated his concerns about the crosshairs image and gave Mr. Tweedt a detailed description of the image and the accompanying language. Upon reading Mr. Kirby's detailed description, Mr. Tweedt emailed Mr. Kirby that the image was actually the logo for the "rap group" Public Enemy. See Ex. G.
- 7. On October 8, 2015, Ms. Tuttle left report on Mr. Tweedt's office chair.
- 8. On October 12, 2015, upon his return from out of town travel, Mr. Tweedt reviewed the report.
- 9. On October 13, 2015, Mr. Tweedt gave the report to Mr. Boss, who at some point thereafter gave the report to Attorney General Ellen Rosenblum.
- 10. On October 20, 2015, the Attorney General called Mr. Tweedt into a meeting with herself and Mr. Boss, during which she expressed her extreme displeasure over the report by because she believed he had engaged in racial profiling. She instructed Mr. Tweedt to find anti-racial profiling training for the Special Agents, and ordered that all SMMS use be immediately discontinued.



⁸ Note that none of Mr. Johnson's tweets that were attached to October 1, 2015 memo contained any reference to "fuck the police."

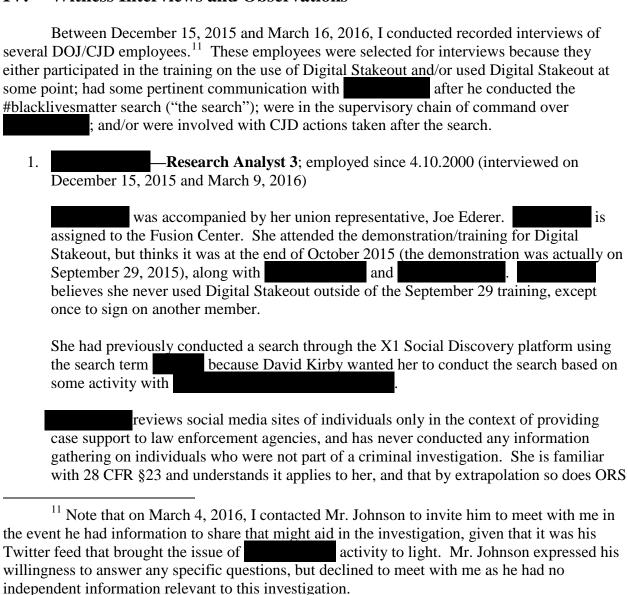
- 11. On or about October 20, 2015, at the direction of Mr. Tweedt, Steve McIntosh verbally notified some employees to discontinue use of Digital Stakeout. It is unclear whether he notified all of the employees at that time, as there are conflicting accounts of who received this verbal notice and when it was received.
- 12. On November 10, 2015, was placed on administrative leave pending the outcome of this investigation.
- 13. On November 12, 2015, Mr. McIntosh sent an email to all subject employees to discontinue use of Digital Stakeout. See Ex. H.
- 14. All other employees, except had stopped any active use of Digital Stakeout at or before the time Mr. McIntosh issued his November 12, 2015 email.
- 15. The trial version of Digital Stakeout that was being used by employees was not enabled to keep a record of searches conducted by employees, so the search terms could not be verified independently from the list provided to this investigator that the employees reported having used.⁹
- 16. Digital Stakeout allows users to access only open source (publicly available) information, and does not allow users to breach information that is protected by privacy settings. None of the searches conducted by and other employees using Digital Stakeout accessed non-public information on Mr. Johnson or others.
- 17. Mr. Johnson was not specifically targeted for investigation by
- 18. Conducted the search of the terms that resulted in finding Mr. Johnson's Twitter posts of his own volition, and not under any direct or implied orders of the DOJ.
- 19. The Intelligence Unit is subject to federal 28 CFR Part 23 regarding Criminal Intelligence Systems Operating Policies and to its state equivalent, ORS §181.575 (now recodified as ORS §181A.250), as well as the unit's own policies regarding privacy and free speech rights of individuals and groups. These policies apply regardless of whether the information being gathered or sought is obtained while engaged in a training exercise or while conducting substantive work.
- 20. search was not in compliance with 28 CFR Part 23, ORS §181.575 or the Intelligence Unit's Privacy Policy. 10
- 21. Once conducted the search, the lack of a diverse or alternative point of view regarding the import of the search results contributed to the belief that Mr. Johnson's posts constituted a potential threat to the police.
- was verbally directed to prepare a written memo based on his description of the search results and his belief that the posts constituted a potential threat to police.
- 23. Intelligence Unit employees either are not uniformly provided with copies of all relevant departmental policies, or do not recall having received all such policies.

⁹ The combined list of search terms any of the employees reported using is included in a November 9, 2015 email from Mr. McIntosh to Mssrs Tweedt and Kirby and Stephanie Tuttle. See Ex. I.

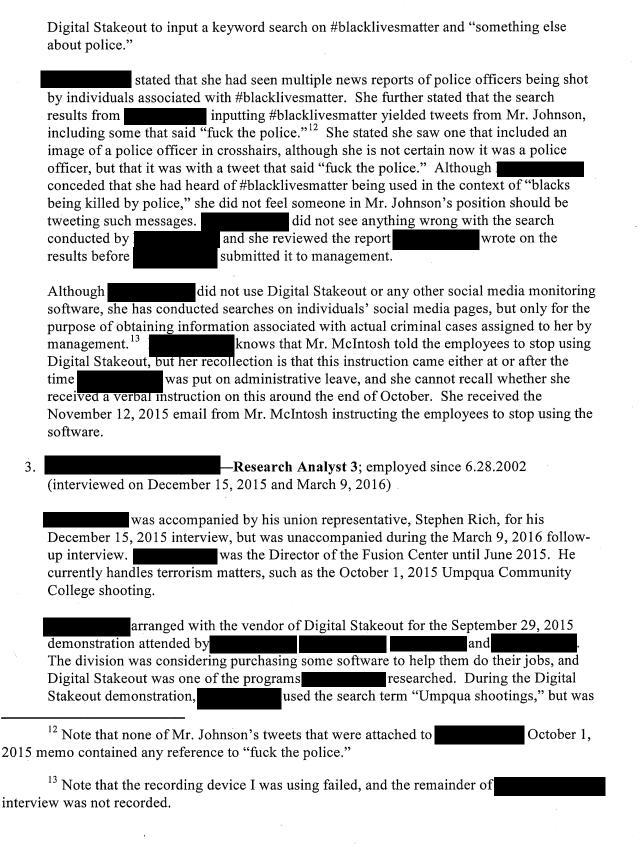
Depending on whether he obtained prior written authorization from a superior, actions may also be out of compliance with the Social Media Non-Covert Investigation Policy 3-101.5.

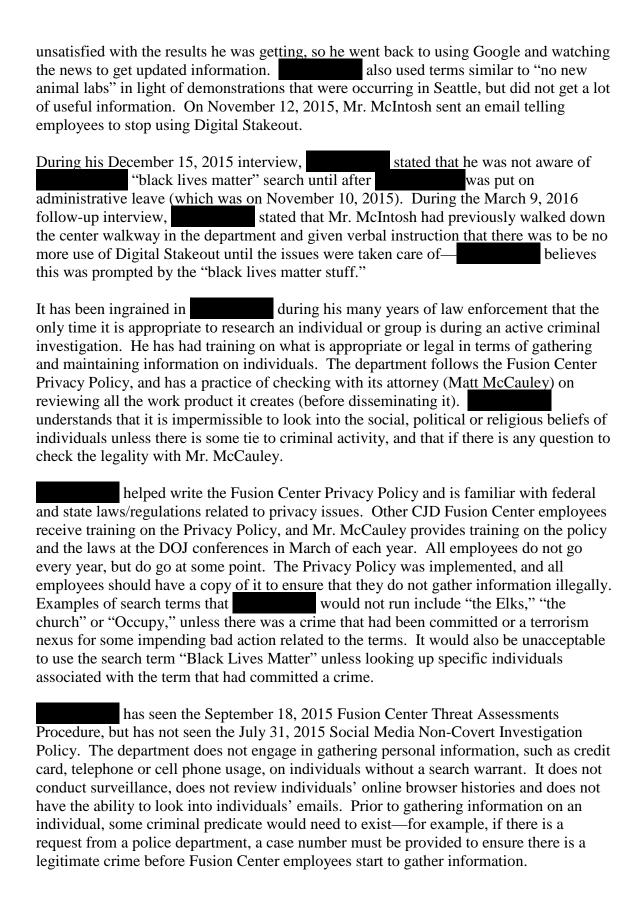
- 24. Intelligence Unit employees are either not receiving or taking advantage of relevant training offered on applicable laws and departmental policies on a consistent basis.
- 25. Intelligence Unit employees have not received adequate cultural competency training, or training on anti-racial profiling, hidden or implicit bias, and/or diversity training.
- 26. The Intelligence Unit is in the process of updating its policies and training procedures and implementing a system to maintain the policies and more consistently mandate and track the training.
- 27. The Intelligence Unit has taken steps to implement anti-racial profiling training for its employees and plans to move forward with the training pending the outcome of this investigation.

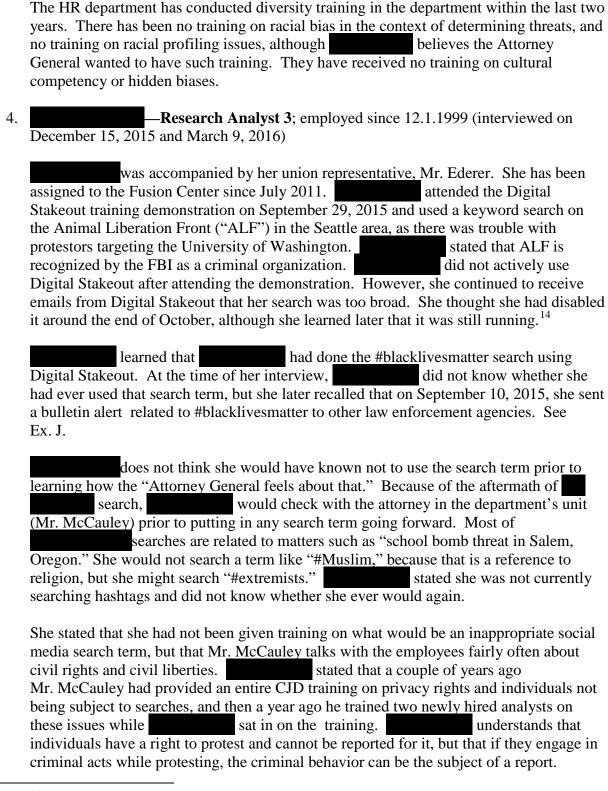
IV. Witness Interviews and Observations



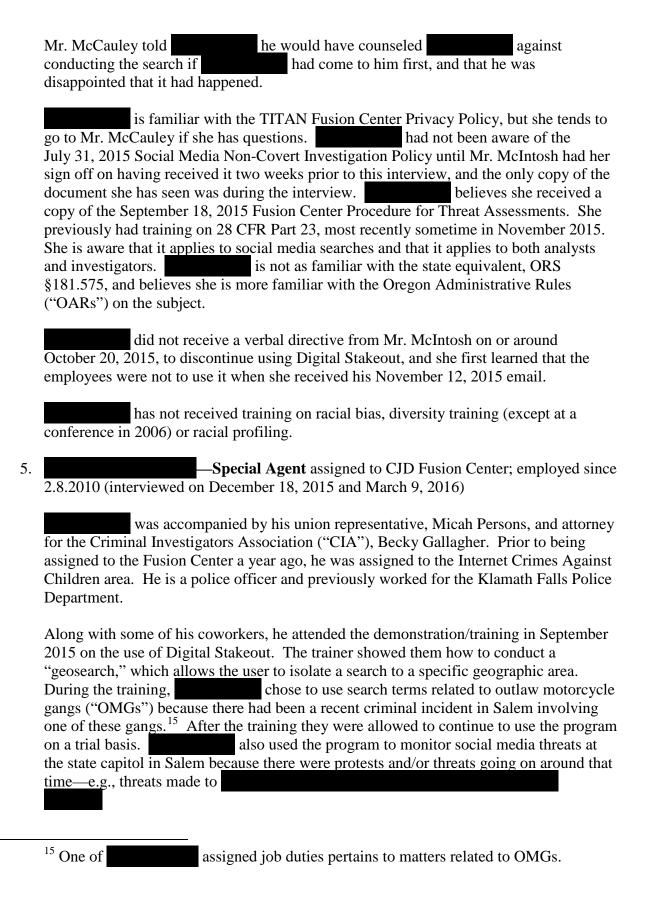
§181.575. She is unfamiliar with the September 18, 2015 Fusion Center Procedure for Threat Assessments, and she does not typically conduct threat assessments. When threat assessments are conducted, the assessment is targeted toward an event (such as the Hillsboro Air Show) to determine whether the event is subject to a threat, rather than conducting an assessment to determine whether a particular individual is considered a threat. She is familiar with the Fusion Center Privacy Policy and has received formal online training within the last year on some of the information contained therein. does not have the ability to access emails of individuals, which requires a subpoena. She does not conduct surveillance in her position, and does not know whether individuals whom she has conducted research on based on a law enforcement request are subjected to surveillance after she submits her search results to law enforcement. attended the September 29, 2015 vendor demonstration/training on Digital Stakeout along with others in her department. Sometime after the training, a map location with a "dot on it," which represented the building they were in, but she does not recall the search terms he used to obtain that geographical location result. expressed surprise that someone in the building was expressing views that felt presented an officer safety issue. The next time she heard anything about the search conducted was when it came out in the was told verbally (she believes sometime in September or October) that the department could no longer use Digital Stakeout or other social media monitoring platforms by either David Kirby, Steve McIntosh or another employee, and also later received a November 12, 2015 email from Mr. McIntosh that they were to discontinue use. At the time was put on administrative leave (November 10, 2015), was not using the software at all to conduct searches. has been trained on 28 CFR §23 and recognizes there are some search terms that would be inappropriate, such as conducting a search based on a person's religion, political views/party affiliation, race or sexual orientation, etc. She is not aware of anyone in her department conducting such searches. has not been given any training on racial bias, hidden biases or racial profiling, but has had diversity training in the past. —**Research Analyst 3**; employed since 6.12.2006 (interviewed on December 15, 2015 and March 9, 2016) was accompanied by her union representative, Mr. Ederer. has been assigned to the Fusion Center since October 1, 2015 and prior to that was an analyst assigned to the High Intensity Drug Trafficking Areas ("HIDTA"). She is familiar with Digital Stakeout, and she was given access to it although she never used it and did not attend the September 29, 2015 demonstration provided by the vendor. showed how the "geofence" component on Digital Stakeout worked on the computer in his office either on September 29 or 30, 2015. The next day, showed on his computer a search he had conducted using

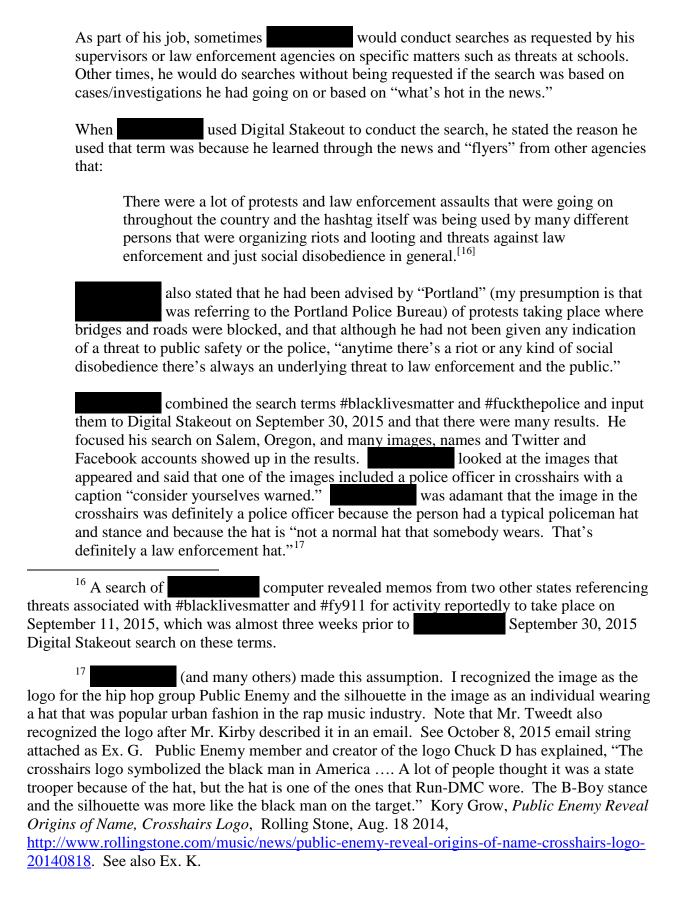


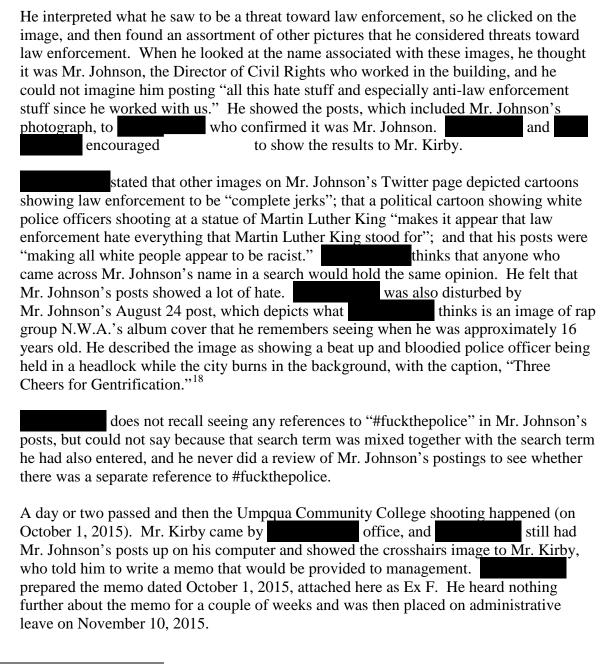




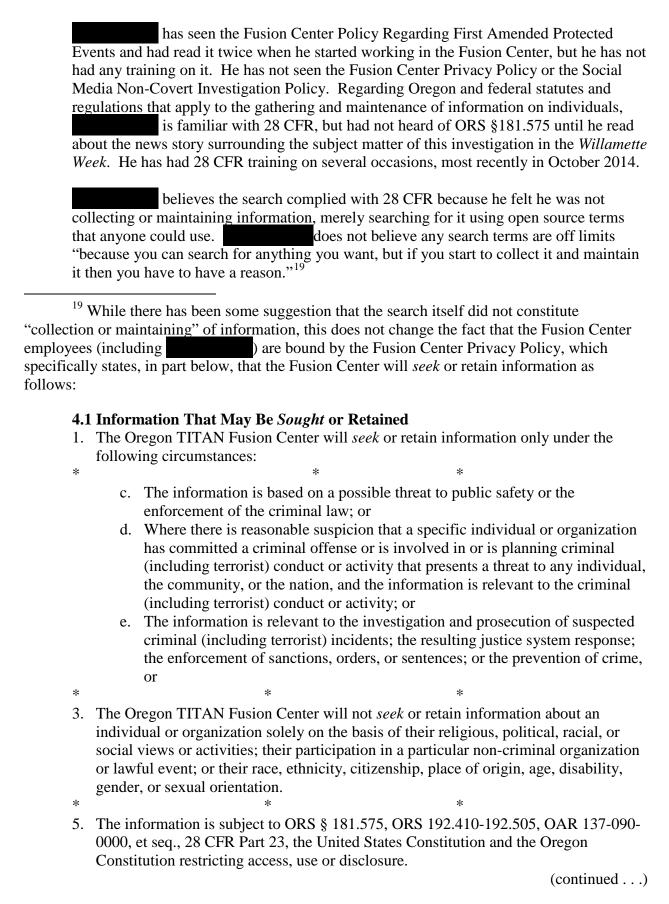
¹⁴ Digital Stakeout allows a user to create an ongoing search that will continue even after logging out of the system until the user disables the ongoing search.



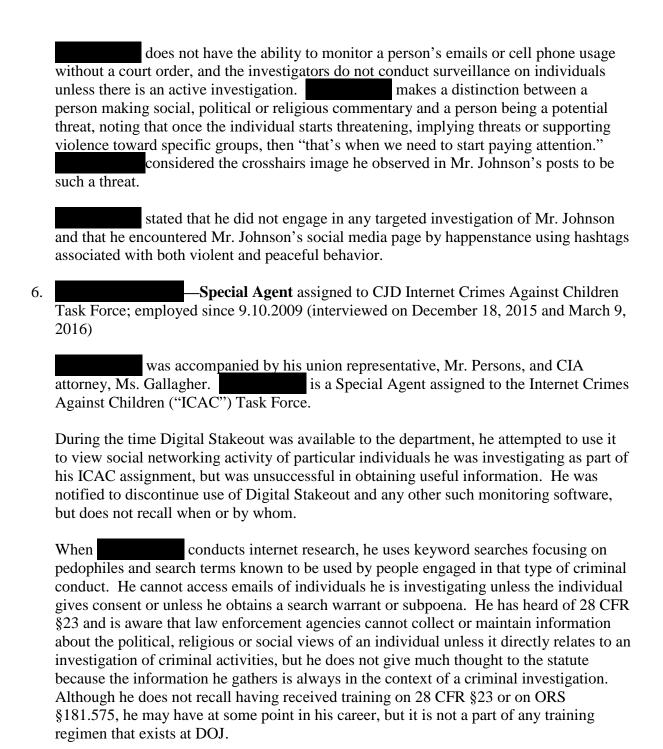




¹⁸ I am unaware of any such N.W.A. album cover. The image is actually a photograph of a painting that hangs in the Know bar on Alberta Street in Portland, Oregon. The neighborhood where the Know is located is widely recognized as a gentrified neighborhood, and the bar is a punk/rock bar. It appears that rather than a post meant to celebrate violence directed at police officers, Mr. Johnson's caption, "Three Cheers for Gentrification," may have been intended as an ironic comment about the content of the art work hanging in a punk bar located in a gentrified Portland neighborhood. Comments about this post, the crosshairs post and other of Mr. Johnson's posts demonstrates a possible lack of cultural awareness that may have affected his perception and led him to experience a heightened sense of concern.

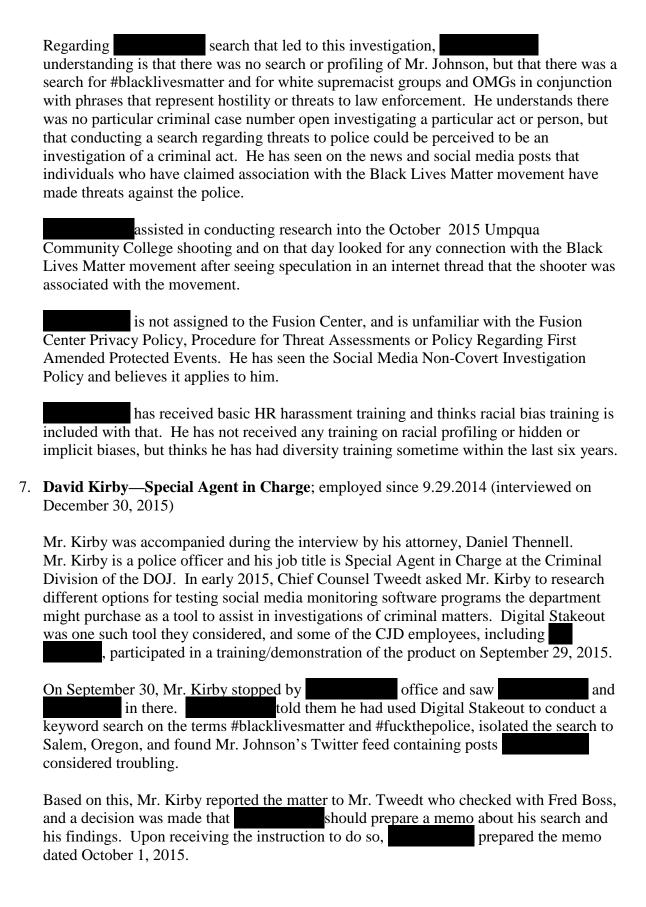


	stated he has had training regarding racial bias through law diversity classes and the military, as well as when he was with the Klamath Falls Police Department. In mid-September 2005, he had such training through DOJ's HR department. He has received no anti-racial profiling training, and although he recalls receiving some kind of information in class regarding recognizing what would be considered racial profiling, he does not recall the class, any specifics about it or how long ago he took the class. He received some cultural competency training when he was in the military and with the police department, but he has not had any such training since coming to the DOJ. He has not had any training on implicit or hidden bias.
	does not believe the search was inappropriate because "it was a hot topic at the time that was causing riots and people getting injured and killed and public destruction." He felt the search was no different from a search on OMGs or Volksfront, because #blacklivesmatter is simply a hashtag used by a wide assortment of people to do a wide assortment of things, one of which is to promote violence. ²⁰
	During the December 18, 2015 interview, stated he had never been told to stop using Digital Stakeout, and that he continued using the program until he was placed on administrative leave on November 10, 2015. However, during the follow-up March 9, 2016 interview, stated that he had been directed to stop using the program by Mr. McIntosh shortly after he generated his October 1, 2015 memo, and that he had actually stopped using it even before Mr. McIntosh's instruction. did not explain his earlier contradictory statements. ²¹
cor	ntinued)
Oregon	TITAN Fusion Center Privacy Policy, at 3-4 (italics added).
Volksfr repatri gang vi ouild co lialogu	It is concerning that sees no distinction in this regard between ont, a group founded on the premise of white supremacy and a reported goal to ate minorites"; OMGs, which are known to engage in drug trafficking, crime rings, theft, olence, etc.; and #blacklivesmatter, which is a self-described, "online forum intended to onnections between Black people and our allies to fight anti-Black racism, to spark e among Black people, and to facilitate the types of connections necessary to encourage ction and engagement." See http://blacklivesmatter.com/about/ .
General mmedi followe verbally 2015 er hat the	Note that in the time period between initial December 18, 2015 w and his March 9, 2016 follow up interview, this investigator learned from the Attorney 's office that there was concern that the Attorney General's October 20, 2015 directive to ately discontinue use of SMMS programs was not immediately communicated to and/or d by employees. I therefore questioned some employees on when and whether they were notified of the directive any time prior to having received Mr. McIntosh's November 12, nail. I do not know whether anyone told prior to his follow up interview timing of the implementing the directive and when the employees stopped using SMMS as had become an issue in the investigation.



(... continued)

review the transcript from his initial interview prior to his follow up interview, so his unexplained contradiction undermines his credibility.



Mr. Kirby reviewed the memo, which had Mr. Johnson's Twitter posts attached, and was concerned because his perception at the time was that the image in one of the posts was the silhouette of a police officer in crosshairs. He has since done his own google research on the image, learned that the image was rap group Public Enemy's logo and learned that the image was not a police officer, but a "hip-hop person in a hip-hop pose, with a hat that was worn by a member of" another rap group.

At the time showed Mr. Kirby Mr. Johnson's tweets, Mr. Kirby did not think delving into Mr. Johnson's personal postings was problematic because the search conducted was on open source information, although it may have not been appropriate for to use the search terms he used.

Mr. Kirby thinks that with education and training, he and other police officers within the unit may have had a different perception on what the concerning crosshairs image really was. Mr. Kirby would not have conducted the search conducted because he was not concerned with any activity going on with Black Lives Matter, and he tries to make good decisions about things he does or does not do. He recognizes that Black Lives Matter is a movement and that many people with nefarious agendas that have nothing to do with the movement will join and commit criminal activity, such as what happened with the "Occupy" movement. There are many search terms, such as protected class terms based on race, religion, etc., that would be off limits to Mr. Kirby and his employees.

Mr. Kirby is part of the management team and is in charge of assigning tasks to the investigators and analysts.

assignments include monitoring sovereign citizens, OMGs, individuals making threats on the Attorney General and actual criminal cases.

assignments did not include monitoring or gathering information on threats to police, but if information from another agency regarding threats to the police came in, he would review it and make sure the proper people were aware. Mr. McCauley would then review the information and determine whether it conformed with the law (i.e., 28 CFR and other laws regarding privacy rights) before approving it for further dissemination.

Mr. Kirby can envision as situation in which it would be appropriate for an employee to conduct a search based on a bulletin received from another law enforcement agency, even if there was no ongoing criminal investigation—for example, if they received a bulletin describing a sovereign citizen who threatened to kill a sheriff.

On October 20, 2015, while Mr. Kirby was in Canada conducting active shooter training, he learned during a phone call with Mr. Tweedt and others on the management team that the Attorney General had ordered that the department was to stop using the social media monitoring software. Mr. Kirby understands that Mr. McIntosh then went around the office that day and told the individuals who had been using the software to discontinue doing so. He understands Mr. McIntosh then sent an email on November 12, 2015 with the directive to stop using social media monitoring software.

DOJ analysts and investigators cannot without a search warrant or subpoena obtain or view emails, credit card use, banking and financial information, land or cell phone information, etc. of a private citizen.

Mr. Kirby does not recall whether he has received training on 28 CFR or the state equivalent ORS §181.575, but understands the common sense parameters that you may not target protected classifications. Mr. Kirby is familiar with the Fusion Center Privacy Policy and the Fusion Center Procedure for Threat Assessments. He does not recall the Fusion Center's Policy Regarding First Amendment Protected Events and has not seen the Social Media Non-Covert Investigation Policy.

Since he has been with the DOJ, Mr. Kirby has not received any training on racial bias in the context of doing his work, but he has in the past as a police officer and has received a lot of diversity training during his career. He has not received training per se regarding racial profiling, but has received training on awareness of it, as well as cultural competency and hidden or implicit bias training, when he was working as an officer for Clackamas County.

Mr. Kirby has been in touch with a trainer to provide diversity training for the department that includes a profiling component, and is waiting for approval to proceed with the training.

8. **Darin Tweedt—DOJ Chief Counsel**²²; employed since 2.26.2007 (interviewed on December 30, 2015)

Mr. Tweedt was accompanied by his attorney, Judy Snyder.

The Oregon TITAN Fusion Center Privacy Policy; Social Media Non-Covert Investigation Policy 3-101.5 dated July 31, 2015; and the Fusion Center Procedure for Threat Assessments dated September 18, 2015 apply to all Fusion Center employees.

About a year ago, Mr. Tweedt recognized that there was an intelligence gap in the Fusion Center and HIDTA. To address this, he directed Mr. McIntosh and evaluate social media monitoring software that would allow the user to collect public social media postings with the ability to limit the search to specific terms and geographic areas. This type of program is commonly used by other Fusion Centers around the country, but the Oregon Fusion Center had not yet utilized this type of program. This is how the Digital Stakeout platform came to be tested by certain CJD employees. Some employees also tried out X1 Social Discovery, which has a similar use.

In the Fusion Center and HIDTA, the way an analyst typically gets assigned to a case is when there has been a request for assistance from some other law enforcement agency—

²² At the time I interviewed him, Mr. Tweedt was DOJ Chief Counsel. I understand that his position has since changed and he now serves as a DOJ Assistant Attorney General.

e.g., a police officer from some jurisdiction requesting information on a specific person. The Fusion Center would verify that there was an actual ongoing criminal investigation before agreeing to pull together information for the requestor.

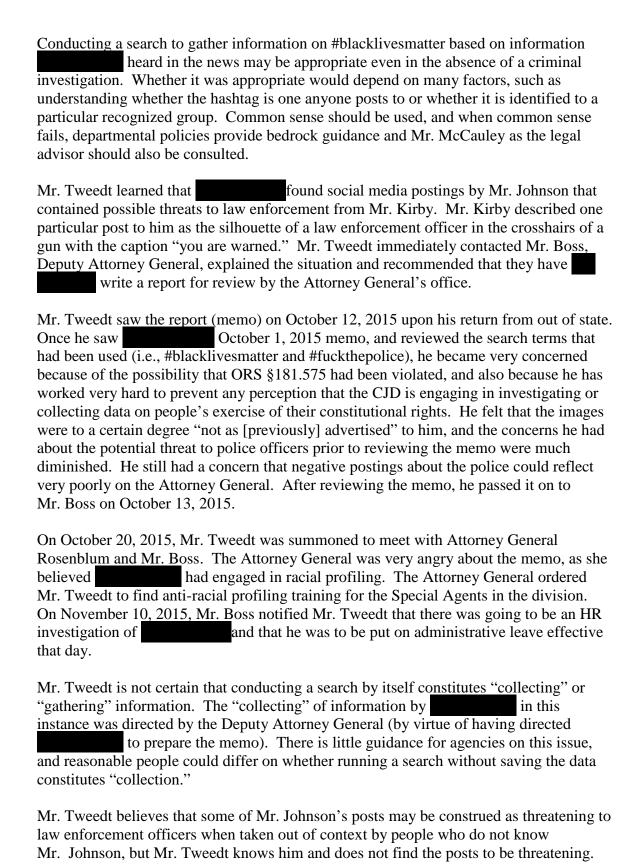
There was no criminal investigation going on with respect to the Digital Stakeout search conducted; rather it was the testing of a computer program. The Fusion Center Privacy Policy, on page 7 at paragraph 4, is instructive in listing the applicable prohibitions (on gathering information). At the time the policy was drafted in 2012, the department was not using social media or social media monitoring tools to the extent they are being used now, but the policy still applies to these more modern standard investigation tools. Mr. Tweedt understands from Mr. McCauley that shortly before conducted the search, attended an annual training by Mr. McCauley that addressed this policy and issues around protected speech.

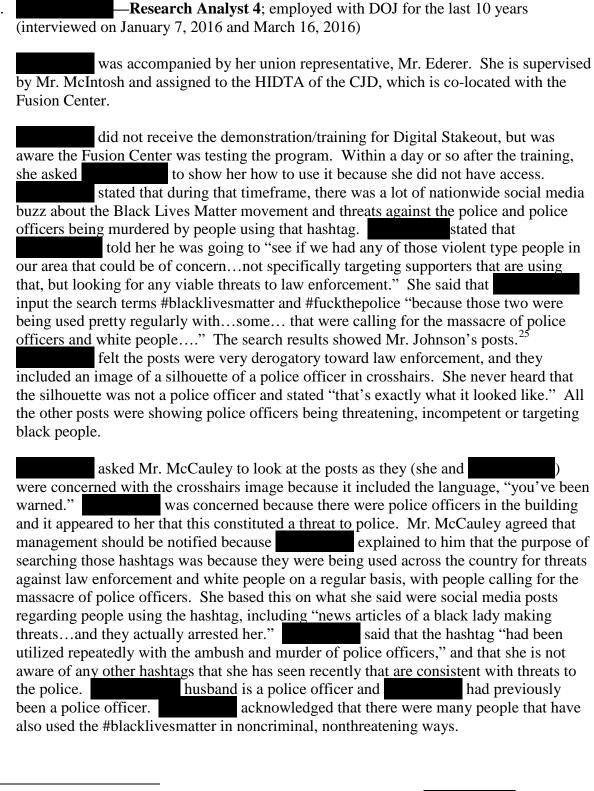
The employees in the department are trained on compliance with 28 CFR and its Oregon equivalent, ORS §181.575, ²³ and the Fusion Center's Privacy Policy is drafted to comply with both. The way an employee would be able to extrapolate from the policy to apply it to social media searches is through training and consultation -- specifically, consultation with Mr. McCauley, whose office is located within the Criminal Intelligence Unit so as to be accessible on a day-to-day basis as a resource to employees to ensure their actions are compliant.

Since becoming Chief Counsel, Mr. Tweedt has been concerned about the Fusion Center and therefore directed his senior level management to begin a complete review of Fusion Center policies. They have since been meeting regularly to review the OARs governing the unit, and have developed draft revised policies that are awaiting review. Mr. Tweedt considers the existing OARs to be out of date. During the process of creating the draft policies, the policy work group has considered many issues that may have addressed the incident involving . Mr. Tweedt has been asked by the Attorney General's office to hold off on further implementation of the revised policies until the matter involving is resolved.

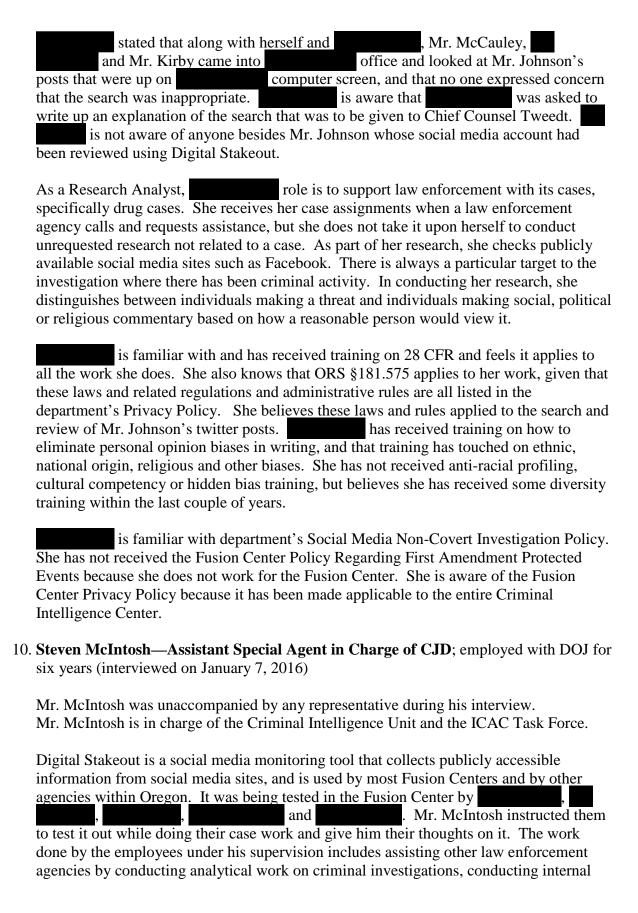
²³ Mr. Tweedt explained that there is a question of whether ORS §181.575 applies to the DOJ based on the wording of §181.575 and the definitions it references in ORS §181.010, but that he believes the Attorney General would certainly determine it applies to the DOJ and to certified law enforcement officers like

²⁴ One of Mr. Tweedt's concerns regarding the Fusion Center was that it was operating in an outdated manner with few written policies that were poorly communicated and were insufficient to address relevant issues. There was also a concern as to what information the Fusion Center should be disseminating as bulletins—for example, in the past, the Fusion Center was prepared to report on groups that were assembling in protest even when there was no report of criminal nexus or public safety concern.





²⁵ Note that none of Mr. Johnson's tweets that were attached to October 1, 2015 memo contained any reference to "fuck the police."



investigations and assisting in requests for threat assessments. Mr. McIntosh has a document he refers to as the Fusion Center Roles and Responsibilities that specifies the tasks and priorities assigned to each of his subordinates.

For any Criminal Intelligence Unit employee to conduct a search for any reason, a reasonable suspicion of a crime must exist, as the employee would not simply do a search on an individual or entity if there is no criminal predicate. This is mandated by the various federal and state data collection laws. Mr. McIntosh does not know whether had a reasonable suspicion when he conducted the search and has not delved any further into it because he was aware this investigation was taking place.

Around September 10, 2015, the Fusion Center issued a report in its weekly bulletin advising that members of #blacklivesmatter and #fy911 social media users were calling for the murder of police officers on a site called Blog Talk Radio. Mr. McIntosh believes this would represent reasonable suspicion of a crime sufficient to warrant a search being done by one of his investigators. The timeframe that the reasonable suspicion would be limited to would be right around September 11, but he cannot give me an exact timeframe. If the report they received included information stating an event was "going to happen yesterday," they would not go any further because the danger would have ended before they were alerted of the problem. The September 10, 2015 Fusion Center report stated that the Fusion Center was not aware of any specific threat directed to Oregon law enforcement, but recommended extreme caution to be exercised "over the weekend" of September 11.

Mr. McIntosh is not aware of any individual besides Mr. Johnson whose social media activity was viewed in this way, and has heard of no employee other than who conducted a search that turned up information on individuals that were not related to a crime. He is unaware of any individuals within the CJD who have done searches that were inappropriate or illegal.

The September 18, 2015 Fusion Center Procedure on Threat Assessments was written and implemented by Mr. McIntosh because the Fusion Center was not keeping good statistics on the threat assessments it was conducting. He disseminated this procedure to employees via email. The Fusion Center's Social Media Non-Covert Investigation Policy was disseminated in July 2015—it describes how social media can be used and applies to the types of investigations conducted by the CJD. This policy requires written supervisor authorization in order to conduct passive viewing of websites. In October or November, 2015, after the incident involving came to light, Mr. McIntosh sent such authorizations to the analysts.

The Fusion Center Privacy Policy was in effect prior to Mr. McIntosh's arrival, and it is in the process of being changed. Mr. McIntosh is also implementing training on the Privacy Policy to be conducted every February.

Mr. McIntosh verbally informed Fusion Center employees to stop using social media monitoring software (including Digital Stakeout) at the end of October and again via email several weeks later.

Mr. McIntosh does not know whether the employees have received any training on racial bias in the context of determining whether and when to gather information. The department received diversity training several years ago. He is not aware of any training the employees received on cultural competency or implicit or hidden bias.

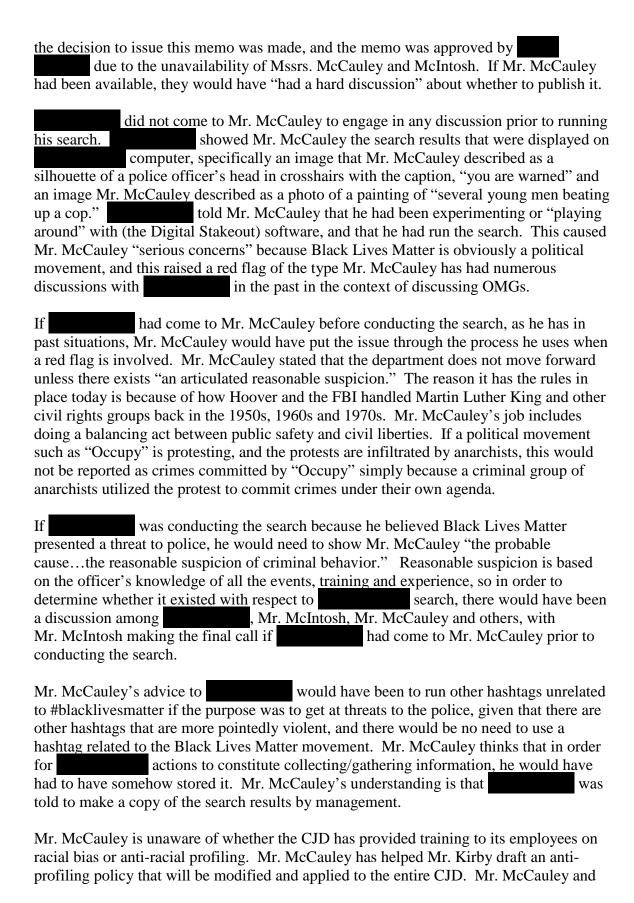
11. **Matt McCauley—Assistant Attorney General**; employed with DOJ for 13 years (interviewed on December 15, 2015)

Mr. McCauley was accompanied by the attorney for the Oregon Association of Justice Attorneys, Jennifer Chapman. Mr. McCauley is assigned to the CJD Criminal Intelligence Center, and half of his assignment involves acting as the legal advisor to the Criminal Intelligence Unit. The Criminal Intelligence Center regularly receives information bulletins from other agencies or jurisdictions and disseminates information to other agencies. Mr. McCauley reviews the information they collect, share, disseminate, store and discard for legal compliance with the OARs, 28 CFR and the Fusion Center Privacy Policy.

Approximately once a year or whenever requested by the Fusion Center, Mr. McCauley also provides training on 28 CFR §23, ORS §181.575 and the Fusion Center Privacy Policy (which Mr. McCauley describes collectively as having slightly different wording of all the same concepts). He gave his last overview on the relevant privacy laws at a law enforcement conference in Bend, Oregon in March of 2015. See email and attached training materials, attached as Ex. L. This conference was attended by

Mr. McCauley regularly instructs the CJD Criminal Intelligence Center employees to come to him whenever they encounter "red flags" in the course of gathering information—i.e., any information that affects the protected class for which there may be a question on whether there is reasonable suspicion of a crime. For example, if a bulletin came in from another state's Fusion Center and the employee sees a "red flag" issue, the employee will come to Mr. McCauley and Mr. McCauley will ask targeted questions to determine whether the information complies with the law and the department's rules.

Mr. McCauley recalls that the Fusion Center in the past received requests for information from other agencies related to Black Lives Matter, but that the Fusion Center did not issue any reports specific to Black Lives Matter because there was no probable cause in Oregon of anybody associated with the movement committing a crime. Mr. McCauley acknowledged that there was a report issued from the Fusion Center on around September 10, 2015 advising that members of #blacklivesmatter and #fy911 social media users were calling for the murder of police officers on a site called Blog Talk Radio. The report noted that the Fusion Center was not aware of any specific threat directed to Oregon law enforcement, but recommended extreme caution to be exercised "over the weekend" of September 11. Mr. McCauley was in court and unavailable when



Mr. McIntosh are planning to conduct annual training for every employee in the Criminal Intelligence Unit on all the policies, including the racial profiling policies that are being developed. Mr. McIntosh has drafted a policy regarding the use of social media tools within the Criminal Intelligence Center, and the goal was to have this policy disseminated by January 1, 2016.

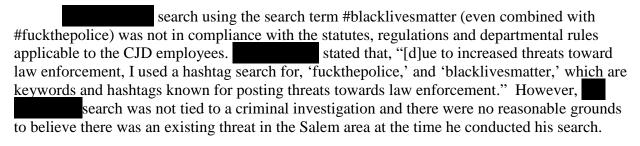
V. Conclusions and Recommendations

Based on my investigation to date, I do not believe there is widespread behavior/actions by CJD Intelligence Unit employees like that engaged in by regarding his search of #blacklivesmatter postings. It appears to have been an isolated incident prompted by the testing of the software Digital Stakeout, and I do not believe that a further department-wide internal audit into employees' searching for information on individuals or groups is necessary.

The Intelligence Unit employees have varying levels of understanding whether 28 CFR § 23 applies to the CJD investigators/analysts, although most seem to accept that it does. The employees also have varying levels of knowledge/awareness of ORS §181.575 (now recodified as ORS §181A.250). Despite the fact there has been training given as recently as March 2015 on the applicability of these statutes to the employees, not all have attended or recollect the training.

Some employees questioned whether 28 CFR § 23 and ORS § 181.575 apply to the CJD investigators/analysts in conducting open source internet searches and whether such a search alone constitutes "collecting" or "maintaining" data if the search is not saved or printed out. Assuming *arguendo* that the statutes do not apply to a simple Google search, for example, I think the argument fails when applied to a SMMS program like Digital Stakeout. The very nature and presumably the most beneficial use of Digital Stakeout is that it searches various social media sites and *gathers* or *collects* the data into a single onscreen location/format that can then be accessed by the user of the product. Information, "such as screen name, hashtags, mentions, urls, generator and content type are automatically extracted and *stored* as [searchable] fields" on the user's computer screen.

In any event, the CJD privacy/first amendment policies are sufficiently clear to suggest that such a *search* is not acceptable unless based upon a possible public safety threat or reasonable suspicion that an individual or organization has committed or is planning to commit a crime.



²⁶ See http://www.digitalstakeout.com/threat-intelligence-platform (italics added).

may assert that along with news media reports from other parts of the country, he relied on bulletins received from other law enforcement agencies that alerted CJD employees of threats associated with #blacklivesmatter. I obtained copies of such bulletins from a search of computer. The bulletins I reviewed came from two intelligence agencies outside the state of Oregon within the week leading up to September 11, 2015. These bulletins addressed perceived threats of protests and violence to take place specifically targeted to September 11, 2015 that were alleged to have been made on a site called blog radio. The bulletins asserted that these threats were associated with the terms #blacklivesmatter and #fy911, among others.²⁷ I did not find any post-September 11, 2015 bulletins that contained such warnings.

did not conduct his search until September 30, 2015, almost three weeks after the September 11 target date. Further, according to Mr. McCauley, told him he was just playing around with the software to see what it could do, as opposed to conducting a search related to an active criminal investigation. The search results yielded Twitter posts made by Mr. Johnson. However, Mr. Johnson had not made any threats, and rather appears to have been expressing his dissatisfaction with incidents of police shootings of or biased behavior toward African Americans. Rather than depicting threats to the police, the majority of the law enforcement related posts by Mr. Johnson appear to be satirical cartoon images depicting threats from the police toward African Americans. These postings are protected by Mr. Johnson's First Amendment rights to free speech. Thus there should have been no continued viewing, documentation, sharing with others or any other action based on the tweets.

Based on the description by to his supervisors of Mr. Johnson's postings constituting violent threats toward police officers, and based on the lack of recognition by and others of an alternative point of view of what postings actually depicted or represented, it is not surprising that he was directed to prepare a memo on the matter.

There is a lack of training on anti-racial profiling ²⁸ and/or anti-bias in the workplace as applied to law enforcement/support activities. Further, there appears to be a lack of racial

²⁷ Note that these bulletins contained privacy statements generally prohibiting their dissemination, so I have not attached them to this report.

The American Civil Liberties Union ("ACLU") describes racial profiling as follows: "Racial Profiling' refers to the discriminatory practice by law enforcement officials of targeting individuals for suspicion of crime based on the individual's race, ethnicity, religion or national origin." Oregon House Bill 2002, signed into law on January 2015, directs law enforcement agencies to adopt written policies and procedures prohibiting profiling by January 1, 2016 (note, this requirement was not in effect at the time of the incident that led to this investigation and is being included herein for the purpose of providing the definition of profiling under Oregon law). Under Oregon law, profiling is described as when "a law enforcement agency or a law enforcement officer targets an individual for suspicion of violating a provision of law based solely on the real or perceived factor of the individual's age, race, ethnicity, color, national origin, language, gender, gender identity, sexual orientation, political affiliation, religion, (continued . . .)

diversity and cultural competency within the CJD that may have contributed to the situation that prompted this investigation. The CJD should proceed with the Attorney General's directive to provide anti-racial profiling to the Intelligence Unit, and should implement mandatory training in the related and often overlapping areas of diversity, cultural competency and anti-bias training. The CJD should also focus on increasing the racial and ethnic diversity within the Intelligence Unit.

The Intelligence Unit as a whole would benefit from clear and consistent leadership and direction regarding applying the relevant statutes and regulations to their daily activities, specifically with respect to electronic monitoring of social media. This training should be mandatory, documented and monitored for compliance, and refresher training should be provided at scheduled intervals.

(... continued)

homelessness or disability, unless the agency or officer is acting on a suspect description or information related to an identified or suspected violation of a provision of law."