



## **An Internal Report on Oregon's Illegal Surveillance of Black Lives Matter on Twitter Leaves Us With More Questions Than Answers** <sup>[1]</sup>

### **Author(s):**

David Rogers

*This blog originally appeared on the ACLU of Oregon's [website](#)* <sup>[2]</sup>.

Last week a [report](#) <sup>[3]</sup> on the surveillance of Black Lives Matter in Oregon was released by the Oregon Department of Justice.

The report confirmed what we learned back in November: That an agent who works for the Criminal Division of DOJ was testing a surveillance program, called Digital Stakeout, by searching various key words, including #BlackLivesMatter. The agent then mistook posts from DOJ's own director of civil rights, including a post of the logo of the legendary hip-hop group Public Enemy and political cartoons, as a threat to law enforcement and wrote a memo that was passed all the way up the chain of command to Attorney General Ellen Rosenblum before it was, finally, rejected as dangerous, racial profiling. The attorney general hired an outside attorney to conduct an independent investigation of the matter to determine if policies or laws were violated.

In other words, the law that prohibits law enforcement from surveilling innocent Oregonians was broken.

After reading through the report and looking through the [exhibits](#) <sup>[4]</sup>, we are left with more questions than answers. I honestly don't know whether to laugh or to cry at the lack of awareness that was revealed of both the law and of what might constitute a threat. This is not only shameful, but also dangerous. Given the power that they wield, I am dismayed at the state of the Criminal Justice Division and afraid for the Oregonians that are supposed to be protected by them. Self-reinforced bias — against protesters, black people, and who knows who else — has left the agency ill-equipped to do their job.

While the report falls short in several areas, one thing it does conclude is that this agent was "not in compliance" with state law. In other words, the law that prohibits law enforcement from surveilling innocent Oregonians was broken.

We still do not know who else was caught up in this illegal dragnet. From the little we have learned, it doesn't seem possible that this was an isolated incident when it is clear that there is a fundamental misunderstanding of the law. Not only is this ineffective law enforcement. It will also have a chilling effect on free speech and assembly, as Oregonians will rightfully wonder whether they are also being monitored. If the attorney general's office is getting it wrong — when they are the ones charged with enforcing the laws of Oregon — then we must assume that other law enforcement are engaging in illegal surveillance too.

This glimpse into the inner workings of the Oregon Department of Justice has revealed severe problems. Attorney General Rosenblum has a formidable task ahead of her to fix these problems and to regain the public's trust.

*This post is part of a series exploring what we have learned about the DOJ surveillance of Black Lives Matter in Oregon. [Click here](#) [2] to see all of our posts on this topic.*

© 2015 ACLU

**Source URL:** <https://www.aclu.org/blog/speak-freely/internal-report-oregons-illegal-surveillance-black-lives-matter-twitter-leaves-us>

#### Links

- [1] <https://www.aclu.org/blog/speak-freely/internal-report-oregons-illegal-surveillance-black-lives-matter-twitter-leaves-us>
- [2] <http://aclu-or.org/blog>
- [3] [http://aclu-or.org/sites/default/files/DOJ\\_Investigation\\_Final\\_Redacted\\_Report.pdf](http://aclu-or.org/sites/default/files/DOJ_Investigation_Final_Redacted_Report.pdf)
- [4] [http://aclu-or.org/sites/default/files/DOJ\\_Investigation\\_Final\\_Redacted\\_Exhibits.pdf](http://aclu-or.org/sites/default/files/DOJ_Investigation_Final_Redacted_Exhibits.pdf)

# **INVESTIGATION REPORT**

**Submitted April 6, 2016**

**by**

**Carolyn D. Walker, Attorney  
Stoel Rives LLP**

## Table of Contents

I.	Background .....	1
	Criminal Intelligence Unit.....	1
II.	Investigation Methodology .....	3
III.	Findings.....	4
IV.	Witness Interviews and Observations.....	7
	1. [REDACTED]—Research Analyst 3.....	7
	2. [REDACTED]—Research Analyst 3.....	8
	3. [REDACTED]—Research Analyst 3 .....	9
	4. [REDACTED]—Research Analyst 3 .....	11
	5. [REDACTED]—Special Agent.....	12
	6. [REDACTED]—Special Agent.....	17
	7. David Kirby—Special Agent in Charge.....	18
	8. Darin Tweedt—DOJ Chief Counsel.....	20
	9. [REDACTED]—Research Analyst 4 .....	23
	10. Steven McIntosh—Assistant Special Agent in Charge of CJD.....	24
	11. Matt McCauley—Assistant Attorney General.....	26
V.	Conclusions 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, [REDACTED], 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 [REDACTED] 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 [REDACTED] on administrative leave pending the outcome of the investigation.

[REDACTED] 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.<sup>1</sup> The Criminal Intelligence Unit, aka

---

<sup>1</sup> 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.

(continued . . .)

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.

- Oregon TITAN Fusion Center: 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.<sup>2</sup> This staff works in conjunction with federal, state and local law enforcement agencies. The Fusion Center produces threat assessments<sup>3</sup>, 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.

- High Intensity Drug Trafficking Area (HIDTA) Investigation Support Center: 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).

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

<sup>3</sup> 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."

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

- High Intensity Drug Trafficking Area (HIDTA) Watch Center: The Watch Center's primary mission is to enhance officer safety through deconfliction<sup>4</sup> 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.<sup>5</sup>

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.<sup>6</sup> 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.

---

<sup>4</sup> 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.

<sup>5</sup> Mr. Slauson has since assumed the position of Acting Chief Counsel of the CJD.

<sup>6</sup> 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 [REDACTED] 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 [REDACTED] 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:

- Oregon TITAN Fusion Center Privacy Policy. See Ex. B.
- Social Media Non-Covert Investigation Policy 3-101.5 dated July 31, 2015. See Ex. C.
- Fusion Center Procedure for Threat Assessments dated September 18, 2015. See Ex. D.
- 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.<sup>7</sup>
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.<sup>8</sup>
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.

---

<sup>7</sup> Another SMMS program that was being considered for use by the Intelligence Unit was X1, but it appears to only have been used on a very limited basis by Research Analyst ██████ to conduct a keyword search on the word ██████ based on some activity with ██████

<sup>8</sup> 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, [REDACTED] 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 [REDACTED], 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.<sup>9</sup>
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 [REDACTED] 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 [REDACTED] or the DOJ.
18. [REDACTED] 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. [REDACTED] search was not in compliance with 28 CFR Part 23, ORS §181.575 or the Intelligence Unit's Privacy Policy.<sup>10</sup>
21. Once [REDACTED] 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.
22. [REDACTED] 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.

---

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

<sup>10</sup> Depending on whether he obtained prior written authorization from a superior, [REDACTED] 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

Between December 15, 2015 and March 16, 2016, I conducted recorded interviews of several DOJ/CJD employees.<sup>11</sup> These employees were selected for interviews because they either participated in the training on the use of Digital Stakeout and/or used Digital Stakeout at some point; had some pertinent communication with [REDACTED] after he conducted the #blacklivesmatter search ("the search"); were in the supervisory chain of command over [REDACTED]; and/or were involved with CJD actions taken after the search.

1. [REDACTED]—**Research Analyst 3**; employed since 4.10.2000 (interviewed on December 15, 2015 and March 9, 2016)

[REDACTED] was accompanied by her union representative, Joe Ederer. [REDACTED] is assigned to the Fusion Center. She attended the demonstration/training for Digital Stakeout, but thinks it was at the end of October 2015 (the demonstration was actually on September 29, 2015), along with [REDACTED] and [REDACTED]. [REDACTED] believes she never used Digital Stakeout outside of the September 29 training, except once to sign on another member.

She had previously conducted a search through the X1 Social Discovery platform using the search term [REDACTED] because David Kirby wanted her to conduct the search based on some activity with [REDACTED].

[REDACTED] reviews social media sites of individuals only in the context of providing case support to law enforcement agencies, and has never conducted any information gathering on individuals who were not part of a criminal investigation. She is familiar with 28 CFR §23 and understands it applies to her, and that by extrapolation so does ORS

---

<sup>11</sup> Note that on March 4, 2016, I contacted Mr. Johnson to invite him to meet with me in the event he had information to share that might aid in the investigation, given that it was his Twitter feed that brought the issue of [REDACTED] activity to light. Mr. Johnson expressed his willingness to answer any specific questions, but declined to meet with me as he had no independent information relevant to this investigation.

§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, ██████████ showed ██████████ 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 media. ██████████ 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.

2. ██████████—**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

Digital Stakeout to input a keyword search on #blacklivesmatter and "something else about police."

██████████ stated that she had seen multiple news reports of police officers being shot by individuals associated with #blacklivesmatter. She further stated that the search results from ██████████ inputting #blacklivesmatter yielded tweets from Mr. Johnson, including some that said "fuck the police."<sup>12</sup> She stated she saw one that included an image of a police officer in crosshairs, although she is not certain now it was a police officer, but that it was with a tweet that said "fuck the police." Although ██████████ conceded that she had heard of #blacklivesmatter being used in the context of "blacks being killed by police," she did not feel someone in Mr. Johnson's position should be tweeting such messages. ██████████ did not see anything wrong with the search conducted by ██████████ and she reviewed the report ██████████ wrote on the results before ██████████ submitted it to management.

Although ██████████ did not use Digital Stakeout or any other social media monitoring software, she has conducted searches on individuals' social media pages, but only for the purpose of obtaining information associated with actual criminal cases assigned to her by management.<sup>13</sup> ██████████ knows that Mr. McIntosh told the employees to stop using Digital Stakeout, but her recollection is that this instruction came either at or after the time ██████████ was put on administrative leave, and she cannot recall whether she received a verbal instruction on this around the end of October. She received the November 12, 2015 email from Mr. McIntosh instructing the employees to stop using the software.

3. ██████████—**Research Analyst 3**; employed since 6.28.2002 (interviewed on December 15, 2015 and March 9, 2016) .

██████████ was accompanied by his union representative, Stephen Rich, for his December 15, 2015 interview, but was unaccompanied during the March 9, 2016 follow-up interview. ██████████ was the Director of the Fusion Center until June 2015. He currently handles terrorism matters, such as the October 1, 2015 Umpqua Community College shooting.

██████████ arranged with the vendor of Digital Stakeout for the September 29, 2015 demonstration attended by ██████████ ██████████ ██████████ and ██████████. The division was considering purchasing some software to help them do their jobs, and Digital Stakeout was one of the programs ██████████ researched. During the Digital Stakeout demonstration, ██████████ used the search term "Umpqua shootings," but was

---

<sup>12</sup> Note that none of Mr. Johnson's tweets that were attached to ██████████ October 1, 2015 memo contained any reference to "fuck the police."

<sup>13</sup> Note that the recording device I was using failed, and the remainder of ██████████ interview was not recorded.

unsatisfied with the results he was getting, so he went back to using Google and watching the news to get updated information. [REDACTED] also used terms similar to "no new animal labs" in light of demonstrations that were occurring in Seattle, but did not get a lot of useful information. On November 12, 2015, Mr. McIntosh sent an email telling employees to stop using Digital Stakeout.

During his December 15, 2015 interview, [REDACTED] stated that he was not aware of [REDACTED] "black lives matter" search until after [REDACTED] was put on administrative leave (which was on November 10, 2015). During the March 9, 2016 follow-up interview, [REDACTED] stated that Mr. McIntosh had previously walked down the center walkway in the department and given verbal instruction that there was to be no more use of Digital Stakeout until the issues were taken care of—[REDACTED] believes this was prompted by the "black lives matter stuff."

It has been ingrained in [REDACTED] during his many years of law enforcement that the only time it is appropriate to research an individual or group is during an active criminal investigation. He has had training on what is appropriate or legal in terms of gathering and maintaining information on individuals. The department follows the Fusion Center Privacy Policy, and has a practice of checking with its attorney (Matt McCauley) on reviewing all the work product it creates (before disseminating it). [REDACTED] understands that it is impermissible to look into the social, political or religious beliefs of individuals unless there is some tie to criminal activity, and that if there is any question to check the legality with Mr. McCauley.

[REDACTED] helped write the Fusion Center Privacy Policy and is familiar with federal and state laws/regulations related to privacy issues. Other CJD Fusion Center employees receive training on the Privacy Policy, and Mr. McCauley provides training on the policy and the laws at the DOJ conferences in March of each year. All employees do not go every year, but do go at some point. The Privacy Policy was implemented, and all employees should have a copy of it to ensure that they do not gather information illegally. Examples of search terms that [REDACTED] would not run include "the Elks," "the church" or "Occupy," unless there was a crime that had been committed or a terrorism nexus for some impending bad action related to the terms. It would also be unacceptable to use the search term "Black Lives Matter" unless looking up specific individuals associated with the term that had committed a crime.

[REDACTED] has seen the September 18, 2015 Fusion Center Threat Assessments Procedure, but has not seen the July 31, 2015 Social Media Non-Covert Investigation Policy. The department does not engage in gathering personal information, such as credit card, telephone or cell phone usage, on individuals without a search warrant. It does not conduct surveillance, does not review individuals' online browser histories and does not have the ability to look into individuals' emails. Prior to gathering information on an individual, some criminal predicate would need to exist—for example, if there is a request from a police department, a case number must be provided to ensure there is a legitimate crime before Fusion Center employees start to gather information.

The HR department has conducted diversity training in the department within the last two years. There has been no training on racial bias in the context of determining threats, and no training on racial profiling issues, although [REDACTED] believes the Attorney General wanted to have such training. They have received no training on cultural competency or hidden biases.

4. [REDACTED]—**Research Analyst 3**; employed since 12.1.1999 (interviewed on December 15, 2015 and March 9, 2016)

[REDACTED] was accompanied by her union representative, Mr. Ederer. She has been assigned to the Fusion Center since July 2011. [REDACTED] attended the Digital Stakeout training demonstration on September 29, 2015 and used a keyword search on the Animal Liberation Front (“ALF”) in the Seattle area, as there was trouble with protestors targeting the University of Washington. [REDACTED] stated that ALF is recognized by the FBI as a criminal organization. [REDACTED] did not actively use Digital Stakeout after attending the demonstration. However, she continued to receive emails from Digital Stakeout that her search was too broad. She thought she had disabled it around the end of October, although she learned later that it was still running.<sup>14</sup>

[REDACTED] learned that [REDACTED] had done the #blacklivesmatter search using Digital Stakeout. At the time of her interview, [REDACTED] did not know whether she had ever used that search term, but she later recalled that on September 10, 2015, she sent a bulletin alert related to #blacklivesmatter to other law enforcement agencies. See Ex. J.

[REDACTED] does not think she would have known not to use the search term prior to learning how the “Attorney General feels about that.” Because of the aftermath of [REDACTED] search, [REDACTED] would check with the attorney in the department’s unit (Mr. McCauley) prior to putting in any search term going forward. Most of [REDACTED] searches are related to matters such as “school bomb threat in Salem, Oregon.” She would not search a term like “#Muslim,” because that is a reference to religion, but she might search “#extremists.” [REDACTED] stated she was not currently searching hashtags and did not know whether she ever would again.

She stated that she had not been given training on what would be an inappropriate social media search term, but that Mr. McCauley talks with the employees fairly often about civil rights and civil liberties. [REDACTED] stated that a couple of years ago Mr. McCauley had provided an entire CJD training on privacy rights and individuals not being subject to searches, and then a year ago he trained two newly hired analysts on these issues while [REDACTED] sat in on the training. [REDACTED] understands that individuals have a right to protest and cannot be reported for it, but that if they engage in criminal acts while protesting, the criminal behavior can be the subject of a report.

---

<sup>14</sup> 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.

Mr. McCauley told [REDACTED] he would have counseled [REDACTED] against conducting the search if [REDACTED] had come to him first, and that he was disappointed that it had happened.

[REDACTED] is familiar with the TITAN Fusion Center Privacy Policy, but she tends to go to Mr. McCauley if she has questions. [REDACTED] had not been aware of the July 31, 2015 Social Media Non-Covert Investigation Policy until Mr. McIntosh had her sign off on having received it two weeks prior to this interview, and the only copy of the document she has seen was during the interview. [REDACTED] believes she received a copy of the September 18, 2015 Fusion Center Procedure for Threat Assessments. She previously had training on 28 CFR Part 23, most recently sometime in November 2015. She is aware that it applies to social media searches and that it applies to both analysts and investigators. [REDACTED] is not as familiar with the state equivalent, ORS §181.575, and believes she is more familiar with the Oregon Administrative Rules ("OARs") on the subject.

[REDACTED] did not receive a verbal directive from Mr. McIntosh on or around October 20, 2015, to discontinue using Digital Stakeout, and she first learned that the employees were not to use it when she received his November 12, 2015 email.

[REDACTED] has not received training on racial bias, diversity training (except at a conference in 2006) or racial profiling.

5. [REDACTED]—**Special Agent** assigned to CJD Fusion Center; employed since 2.8.2010 (interviewed on December 18, 2015 and March 9, 2016)

[REDACTED] was accompanied by his union representative, Micah Persons, and attorney for the Criminal Investigators Association ("CIA"), Becky Gallagher. Prior to being assigned to the Fusion Center a year ago, he was assigned to the Internet Crimes Against Children area. He is a police officer and previously worked for the Klamath Falls Police Department.

Along with some of his coworkers, he attended the demonstration/training in September 2015 on the use of Digital Stakeout. The trainer showed them how to conduct a "geosearch," which allows the user to isolate a search to a specific geographic area. During the training, [REDACTED] chose to use search terms related to outlaw motorcycle gangs ("OMGs") because there had been a recent criminal incident in Salem involving one of these gangs.<sup>15</sup> After the training they were allowed to continue to use the program on a trial basis. [REDACTED] also used the program to monitor social media threats at the state capitol in Salem because there were protests and/or threats going on around that time—e.g., threats made to [REDACTED]  
[REDACTED]

---

<sup>15</sup> One of [REDACTED] assigned job duties pertains to matters related to OMGs.

As part of his job, sometimes [REDACTED] would conduct searches as requested by his supervisors or law enforcement agencies on specific matters such as threats at schools. Other times, he would do searches without being requested if the search was based on cases/investigations he had going on or based on "what's hot in the news."

When [REDACTED] used Digital Stakeout to conduct the search, he stated the reason he used that term was because he learned through the news and "flyers" from other agencies that:

There were a lot of protests and law enforcement assaults that were going on throughout the country and the hashtag itself was being used by many different persons that were organizing riots and looting and threats against law enforcement and just social disobedience in general.<sup>[16]</sup>

[REDACTED] also stated that he had been advised by "Portland" (my presumption is that was referring to the Portland Police Bureau) of protests taking place where bridges and roads were blocked, and that although he had not been given any indication of a threat to public safety or the police, "anytime there's a riot or any kind of social disobedience there's always an underlying threat to law enforcement and the public."

[REDACTED] combined the search terms #blacklivesmatter and #fuckthepolice and input them to Digital Stakeout on September 30, 2015 and that there were many results. He focused his search on Salem, Oregon, and many images, names and Twitter and Facebook accounts showed up in the results. [REDACTED] looked at the images that appeared and said that one of the images included a police officer in crosshairs with a caption "consider yourselves warned." [REDACTED] was adamant that the image in the crosshairs was definitely a police officer because the person had a typical policeman hat and stance and because the hat is "not a normal hat that somebody wears. That's definitely a law enforcement hat."<sup>17</sup>

---

<sup>16</sup> A search of [REDACTED] computer revealed memos from two other states referencing threats associated with #blacklivesmatter and #fy911 for activity reportedly to take place on September 11, 2015, which was almost three weeks prior to [REDACTED] September 30, 2015 Digital Stakeout search on these terms.

<sup>17</sup> [REDACTED] (and many others) made this assumption. I recognized the image as the logo for the hip hop group Public Enemy and the silhouette in the image as an individual wearing a hat that was popular urban fashion in the rap music industry. Note that Mr. Tweedt also recognized the logo after Mr. Kirby described it in an email. See October 8, 2015 email string attached as Ex. G. Public Enemy member and creator of the logo Chuck D has explained, "The crosshairs logo symbolized the black man in America .... A lot of people thought it was a state trooper because of the hat, but the hat is one of the ones that Run-DMC wore. The B-Boy stance and the silhouette was more like the black man on the target." Kory Grow, *Public Enemy Reveal Origins of Name, Crosshairs Logo*, Rolling Stone, Aug. 18 2014, <http://www.rollingstone.com/music/news/public-enemy-reveal-origins-of-name-crosshairs-logo-20140818>. See also Ex. K.