

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES)	
)	
v.)	
)	CASE NO. 1:20-cr-00264-TFH
MICHAEL PETERSON, JR.,)	
)	
Defendant.)	
_____)	

DEFENDANT’S MOTION TO SUPPRESS

Defendant Michael Peterson, by and through undersigned counsel, hereby moves to suppress the identification and tangible items seized in this case, pursuant to the Fourth and Fourteenth amendments to the U.S. Constitution, and Rule 12 of the Federal Rules of Criminal Procedure. In support of this Motion, Mr. Peterson states the following:

STATEMENT OF FACTS

1. On June 1, 2020, members of the United States Park Police (“USPP”) were at Lafayette Park adjacent to the 1600 block of H Street, NW, Washington, DC in response to protests of the death of George Floyd.
2. At 6:30 p.m., thirty minutes before the 7:00 p.m. curfew order by Mayor Muriel Bowser took effect, United States Park Police (“USPP”) and other law enforcement agencies began forcibly clearing protestors from H Street, NW, starting at the Vermont Avenue, NW intersection.
3. USPP attempted to issue warnings over a loudspeaker with the purpose of clearing people out of Lafayette Square Park, however, many individuals—including officers, journalists,

members of the clergy and protestors—were unable to hear them.¹ Even if the protestors had heard the warnings, “the warnings did not inform protestors where to exit or provide a safe escape route that would have enabled them to avoid the approaching officers.”² In fact, several law enforcement entities deployed before the third dispersal warning had been issued.³

4. Nevertheless, the police officers entered H Street and began advancing towards the protestors. Some protestors appeared surprised and confused, and many ran from the area as the officers advanced.⁴ The Bureau of Prisons’ officers fired pepper balls into the crowd of protestors, the USPP SWAT deployed stinger ball grenades, and the Metropolitan Police Department deployed CS gas against the protestors on 17th Street.⁵ All this contributed to the “chaotic” scene.

5. During the time when law enforcement was forcibly clearing H Street, the Criminal Complaint in this case alleges that Mr. Peterson grabbed an officer by the leg and tried to pull him to the ground. ECF 1-1.

6. Shortly after law enforcement had cleared Lafayette Square Park of all protestors, then President Donald Trump “departed the White House and walked into Lafayette Park . . . crossed

¹ Open source videos “appeared to show that protestors in the crowd at the intersection of H and 16th Streets could not clearly hear the warnings. Multiple officers told us they either did not hear the warnings or could not clearly hear the information conveyed in the warnings. One USPP officer told us that given the size and noise level of the crowd, he believed it was unlikely that all protestors could hear the warnings.” Office of the Inspector General, U.S. Dept. of the Interior, “Review of U.S. Park Police Actions at Lafayette Park,” Case No. 20-0563, at 17 (June 2021).

² *Id.* at 27.

³ *Id.* at 28.

⁴ *Id.* at 17.

⁵ *Id.* at 30.

H Street and stood in front of St. John’s Church.”⁶ He held up a Bible for a few moments, and then walked back to the White House.

7. The Criminal Complaint alleges that on June 2, 2020, Officer Sinacore observed on Twitter a link referencing the events that occurred on June 1, 2020 at the White House. Upon examining the link, Officer Sinacore discovered a digital photograph of a man whom he believed to have encountered the day before. He sent the digital photograph to National Capital Region Facial Recognition Investigative Leads System (“NCRFRILS”) for facial recognition analysis.

8. On June 2, a U.S. Secret Service officer recovered a backpack at 1610 H Street, NW. The Secret Service conducted a warrantless search of the backpack and seized a Virginia Identification Card with Mr. Peterson’s name, and a baseball cap. The Virginia Identification Card included a photograph of his face, which the officers allegedly compared with a undisclosed digital photograph. According to the Complaint, Officers decided that the photographs matched.

9. Coincidentally, seven days later, Officer Tomasiello was shown an unidentified digital photograph and identified the subject depicted in the photograph as the subject who he encountered when USPP Officers attempted to arrest him.

10. The Criminal Complaint alleges that on June 9, 2020, USPP Detective Sergeant Holmberg sent the digital photograph to Lieutenant Garcia with the Prince George’s County Park Police. Lieutenant Garcia utilized the NCRFRILS to generate investigative leads based on the digital photograph. The System allegedly identified Mr. Peterson as a “match candidate,” but the Government has not described what that term means nor listed the total number of other “match candidates” who might have also been identified.⁷

⁶ *Id.* at 20.

⁷ Because the specific images used and the software are so critical to a reliability determination, Mr. Peterson has requested detailed information about how NCRFRILS works and copies of the photographs and supposed “matches” that were selected in this case. The evidence in this case is so deeply embedded in NCRFRILS that we cannot provide

11. On May 17, 2021, the Council of Government announced that it is discontinuing use of the NCRFRILS software as of July 1, 2021.

12. Mr. Peterson is charged by indictment with one count of Assault, Resist, Oppose, Impede, Intimidate, or Interfere with Certain Officers or Employees in violation of 18 U.S.C. § 111(a)(1). Mr. Peterson now files this motion to suppress.

ARGUMENT

Mr. Peterson requests that this Court suppresses the identification of Mr. Peterson because the use of NCRFRILS rendered the risk of misidentification unacceptably high. Facial recognition software, like the software used in this case, has not yet been found to be scientifically reliable. The “overall foundational validity of face recognition as a forensic tool, as it is used in a typical U.S. law enforcement investigation . . . has yet to be established through empirical peer-reviewed study.” Garvie Affidavit at ¶ 4 (“Garvie Affidavit”).⁸ Thus, “the reliability of identity evidence produced by face recognition investigative searches overall is not known, highly variable, and can only be understood on a search-by-search basis by examining the choices, biases, motivations, and degree of training of the human in the loop.” *Id.* In other words, the Government cannot demonstrate that the NCRFRILS “matches” in this case meet the standards of scientific reliability established in *Daubert*. The risk of misidentification is therefore unacceptably high and the identification must be suppressed.⁹

a constitutionally effective defense without full disclosures about the technology and results it generated in this case. Mr. Peterson has attached as Exhibit A the June 3, 2021, discovery deficiency letter he sent to the Government, which requests additional information about the facial recognition software that was used in this case.

⁸ The Garvie Affidavit and her CV are attached as Exhibit B.

⁹ Pursuant to its gatekeeper function, this Court should hold a *Daubert* hearing regarding NCRFRILS. *United States v. Law*, 528 F.3d 888, 912 (D.C. Cir. 2008). Accuracy of face recognition systems is in large part determined by the quality and contents of the probe photo submitted to the algorithm. Analysts or the system itself can make adjustments to a photograph, and there is no certification requirement yet for forensic face analysts in the United States. Additionally, testing conducted by the National Institute of Standards and Technology (NIST), demonstrated that some algorithms perform more accurately than others. Garvie Affidavit at ¶ 14. This means that “the make and model of the algorithm used in a given investigation can directly influence the accuracy of the identification.” *Id.* Aside from these

Furthermore, Mr. Peterson moves to suppress all evidence seized during the warrantless search of his backpack, including the photograph that was used in the identification procedure. Because the search and seizure were illegal, the identification that resulted from the use of that photograph should be suppressed as fruit of the poisonous tree.

I. The use of NCRFRILS unacceptably increased the risk of misidentification and this Court should suppress all identification testimony

This Court should suppress the identification of Michael Peterson because the NCRFRILS search led to an identification procedure that was unreliable and unduly suggestive, thus increasing the risk of misidentification. As the Supreme Court has held, “reliability is the linchpin in determining the admissibility of identification testimony.” *Manson v. Brathwaite*, 432 U.S. 98, 114 (1977). The primary evil to be avoided is “a very substantial likelihood of irreparable misidentification.” *Neil v. Biggers*, 409 U.S. 188, 198 (1972) (citing *Simmons v. United States*, 390 U.S. 377, 384 (1968)); *United States v. Johnson*, 452 F.2d 1363 (D.C. Cir. 1971) (witness failed to identify accomplice from photographs until police selected photograph and indicated this was a friend of suspect already identified by witness).

The Supreme Court recognized that an identification procedure may violate due process if it is “unnecessarily suggestive and conducive to irreparable mistaken identification.” *Stovall v. Denno*, 388 U.S. 293, 302 (1967). An identification procedure is so unduly suggestive as to require suppression if it creates a substantial likelihood of irreparable misidentification. *Simmons v. United*

larger scale examples of complex problems with facial recognition software, the software used in this case has been banned from use in the area, further questioning its reliability. *Id.* at ¶ 30. At a *Daubert* hearing the Court would make a determination regarding the use of NCRFRILS and whether this technology unreasonably increased the likelihood of misidentification. If the Court concludes that it did, then the evidence must be excluded.

States, 390 U.S. 377, 284 (1968); *Neil v. Biggers*, 409 U.S. at 198. The dangers of allowing suggestive and unreliable identification procedures are particularly acute:

A major factor contributing to the high incidence of miscarriage of justice from mistaken identification has been the degree of suggestion inherent in the manner in which the prosecution presents the suspect to witnesses for pretrial identification. A commentator has observed that ‘[t]he influence of improper suggestion upon identifying witnesses probably accounts for more miscarriages of justice than any other single factor—perhaps it is responsible for more such errors than all other factors combined.’

United States v. Wade, 388 U.S. 218, 228–29 (1967) (citation omitted). Once some suggestiveness is shown, the reliability of the identification is determined by weighing “the corrupting effect of the suggestive identification” against factors relating to its reliability, *Manson*, 432 U.S. at 114, because “it is the reliability of identification evidence that primarily determines its admissibility.” *Watkins v. Sowders*, 449 U.S. 341, 347 (1981) (citing *Manson*, 432 U.S. at 113-14). The factors relating to its reliability include the witness’s opportunity to observe the perpetrator and degree of attention paid at the time of the offense, accuracy of prior descriptions, level of certainty at the time of the confrontation, and the time between the crime and the identification. *Id.*

An impermissibly suggestive photographic display gives rise to a very substantial likelihood of irreparable misidentification if the Government is unable to show, by clear and convincing evidence, that a subsequent in-court identification is based on a source independent of the photographic display. *United States v. Gambrill*, 449 F.2d 1148, 1153 (D.C. Cir. 1971) (in-court identification was unreliable following a suggestive identification procedure). In making that determination, courts should consider “the prior opportunity to observe the alleged criminal act, the existence of any discrepancy between any pre-line-up description and the defendant's actual description, any identification prior to lineup of another person, the identification by picture of the defendant prior to the lineup, failure to identify the defendant on a prior occasion, and the lapse of

time between the alleged act and the lineup identification.” *United States v. Wade*, 388 U.S. at 241; *Gambrill*, 449 F.2d at 1157 (noting reliability issues in the victim's testimony, including her limited recollection of the assailant’s distinctive features and the lack of other eyewitness identification by which the reliability of the victim’s identification can be gauged).

A. Probe Photo Quality

“The accuracy of face recognition systems is in large part determined by the quality and contents of the probe photo submitted to the algorithm.” Affidavit of Clare Garvie at ¶ 8. As a result, the “less information the probe photo contains about what the subject looks like, the less information the algorithm has to process, the less reliable the resulting identification will be.” *Id.* Moreover, facial recognition software programs are less reliable when the images being compared have different orientations (i.e., one face is looking at the camera and another is not). Brendan F. Klare, *et al.*, *Face Recognition Performance: Role of Demographic Information, Transactions on Information Forensics and Security*, 1789 at 1 (2012) (sources “of errors in automated face recognition algorithms are generally attributed to the well-studied variations in pose, illumination, and express, collectively known as PIE. Other factors such as image quality (e.g., resolution, compression, blur), time lapse (facial aging), and occlusion also contribute to face recognition errors.”)

In the case at bar, the Criminal Complaint states that Twitter provided the images used for the comparison with the probe photo. But these taken “in the field, under real world conditions that are far from ideal. The online video taken during the protests were taken when people were in motion, including running and turning away from the cameras. Moreover, the chaos at the scene, which included smoke, flash bang explosions, and pepper spray further undermines the ability to identify facial characteristics. Finally, the videos were frequently taken from a significant

distance from the protestors who were depicted, and were not necessarily in focus. The protests at Lafayette Square, especially after law enforcement began clearing the area, provided terrible circumstances for obtaining facial images for facial recognition comparisons. See C. Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, (May 16, 2019), <https://www.flawedfacedata.com/>.

B. Race Is an Unacceptably Significant Factor Impacting Reliability

Facial recognition algorithms are less accurate at identifying African Americans than other racial and ethnic groups. Brendan F. Klare, *et al.*, *Face Recognition Performance: Role of Demographic Information*, *Transactions on Information Forensics and Security*, 1789 (2012) (“[T]he performance of three commercial face recognition algorithms were consistent in that they all exhibited lower recognition accuracies on the following cohorts: females, blacks and younger subjects (18 to 30 years old).”). This deficiency in facial recognition systems compounds the problem of racial bias and disparate treatment in the criminal justice system. See *State v. Henderson*, 27 A.3d 872, 926 (N.J. 2011) (requiring the trial court to give an instruction on the unreliability of cross-racial identification whenever it is in issue). The Court should not allow algorithmic racism to infect Mr. Peterson’s case.

C. The Eyewitness Knew the “Match” Photo was Selected by NCRFRILS

Courts have repeatedly held that single photo identification procedures are suggestive. See *Manson v. Brathwaite*, 432 U.S. at 116. If an eyewitness knows that a suspect image they are being shown was selected by the facial recognition software, it may create a false belief that the perpetrator must be depicted in that image. This “confirmation biases in favor of finding a match” may “skew[] the investigation towards merely certifying, rather than independently corroborating, what the face recognition system proposed as a match.” Garvie Affidavit at ¶ 26. This is especially

true when a suspect's photograph is presented on its own to the witness rather than as part of a photo array; when the suspect's photograph is presented with associated information about the suspect's prior arrest history; or when "confidence scores" and algorithms incorrectly suggest mathematical certainty and therefore bias the witness towards accepting the search results as a match. *Id.*

D. Suppression is Required

Even without full information about the software, it is already apparent that

the face recognition search and human confirmation leading to the identification of [Mr.] Peterson lacks clear indicia of reliability, and contains elements that suggest it was not adequately confirmed by additional, independent investigation, or protected from cognitive bias. In this search, while Lieutenant Garcia ran the face recognition search, criminal complaint affiant Detective Robert Freeman acted as a forensic face analyst, visually comparing two images to determine whether they represent the same individual. Since Detective Freeman was aware that a face recognition search took place which identified the Defendant as a possible match candidate, his review was not shielded from confirmation bias towards agreeing with the algorithm's determination rather than conducting an independent biometric review.

Garvie Affidavit at ¶ 28. For the reasons stated above, this identification procedure was unduly suggestive and produced unreliable and potentially biased results. The identification of Mr. Peterson must therefore be suppressed.

II. The Court Must Suppress the Backpack's Contents

The police seized Mr. Peterson's backpack, searched its contents and seized an identification card found in the backpack. The police used a photograph on the identification card to identify Mr. Peterson. Because the search was conducted without a warrant and no exceptions to the Warrant Requirement applied, the contents of the backpack—including the photo—were not seized legally and must be suppressed.

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not

be violated, and no warrants shall issue, but upon probable cause." *See* U.S. CONST. amend. IV. Because warrantless searches are presumed to be unreasonable, law enforcement officers generally must first obtain a judicial warrant before searching a person or a person's property for evidence of criminal wrongdoing. *See Riley v. California*, 573 U.S. 373, 382 (2014).

"Even if an officer has probable cause to believe that a bag (or a box, or a house) contains evidence of criminal activity, he must get a warrant before searching it unless one of the actual exceptions to the warrant requirement applies." *United States v. Wills*, 316 F. Supp. 3d 437, 443-44 (D.D.C. 2018) (*citing United States v. Howard*, 156 F.Supp.3d 1045, 1048 (N.D. Cal. 2016)).

In the case at bar, there is no evidence that Mr. Peterson abandoned his backpack or denied ownership of it. *United States v. Brady*, 842 F.2d 1313, 1315-16 (D.C. Cir. 1988) (prosecution has burden of proving that defendant intended to voluntarily abandon seized drugs). In fact, during the chaos in Lafayette Square he simply lost it. According to the Criminal Complaint, officers recovered the bag and simply began to search it. They then went through its contents, removed an identification card, and then apparently used the digital image from the card for identification purposes. Because the Twitter digital image was insufficient to identify the facial characteristics of the suspect, and the facial recognition searches generated numerous "matches," it is clear that the illegally seized identification card was used impermissibly for the identification of Mr. Peterson. In other words, it appears that the officers recovered the backpack, assumed that Mr. Peterson must have been the suspect, and used the facial recognition software to rationalize their assumption. The entire identification process was hopelessly tainted.

Therefore, the evidence derived from this illegal search and seizure, including the identification procedure, must be suppressed. *See Brown v. Illinois*, 422 U.S. 590, 602-03 (1975).

