SUPREME COURT OF THE STATE OF NEW YORK
[redacted]

THE PEOPLE OF THE STATE OF NEW YORK

-against-

NOTICE OF MOTION TO SUPRESS IDENTIFICATION TESTIMONY OR ALTERNATIVELY FOR WADE AND RELIABILITY HEARINGS, DEMAND FOR DISCOVERY, & OMNIBUS MOTION

[redacted]

Ind. No. [redacted]

Defendant

PLEASE TAKE NOTICE, that Kaitlin Jackson, Esq. has attached a motion and affirmation, and moves this Supreme Court, [redacted] to issue an order [redacted]:

1. Suppressing evidence and testimony relating to identifications of [redacted] (for which the Government served proper notice under C.P.L. § 710.30) or, in the alternative, granting a hearing for findings of fact and conclusions of law (*Wade/ Rodriguez/ Independent Source*);
2. Precluding evidence relating to identifications of [redacted] and expert testimony about the NYPD's use of facial recognition program (called FIS). Or alternatively, **ordering a reliability hearing.** If the Government intends to introduce expert testimony about FIS, then this court should hold a traditional *Frye* hearing. *See Frye v. U.S.*, 293 F. 1013 (D.C. Cir. 1923). If the Government does not intend to introduce expert testimony, then this

court should hold a *Frye-type* hearing to determine whether the use of FIS contributed to an unreasonable risk of misidentification in this particular case;

3. Ordering the Government to **provide discovery regarding FIS** in this case, pursuant to C.P.L. § 240.20;
4. Ordering the Government to **produce *Brady* information related to the FIS procedure** used in this case, including, but not limited to, all other images identified by FIS as possible matches to the submitted image as well as confidence ratings of the matches. See *Brady v. Maryland*, 373 U.S. 83, 87 (1963);

[redacted]

Kaitlin Jackson, Esq.

[redacted]

SUPREME COURT OF THE STATE OF NEW YORK
[redacted]

THE PEOPLE OF THE STATE OF NEW YORK

-against-

AFFIRMATION

[redacted] Ind. No. [redacted]

Defendant

[redacted]

STATEMENT OF FACTS

4. On [redacted], someone stole socks from [redacted]. A loss prevention officer (LPO) approached the sock thief, and the sock thief allegedly displayed a sharp object in his direction. The LPO [redacted] and

the sock thief are not known to each other. The [redacted] store was equipped with surveillance cameras.

5. On [redacted], more than two weeks after the theft, Detective [redacted] submitted some number of screenshots from the surveillance video to be run through the NYPD's facial recognition software. The defense does not know how these screenshots were obtained, how many still images were put into the software, or whether those photos were edited or altered.
6. Assuming the screenshot photo is the same photo that was provided to the defense, the resolution is poor. ***See*** **Exhibit 1**- (*Facial Identification Section Search Result Report*).
7. The next day FIS generated a report and [redacted]s photo as well as other look-a-like photos were listed as possible "matches." ***See*** **Exhibit 1.**
8. The NYPD has not, and does not, release information to the public regarding the technology used by the FIS. *See The Perpetual Line-Up, Unregulated Police Face Recognition in America*, Georgetown Law Center for Privacy & Technology, October 18, 2016[1]; and *NYPD Ripped for Abusing Facial Recognition Tool*, The New York Daily News, March 1, 2018.[2]
9. However, on information and belief, as informed by discussions with experts in the field of facial recognition, and review of available public documents, (FIS) functions in the following manner: at least one image (which may have been altered or edited by a human) is submitted for comparison. The software creates an abstract version of the photo based on certain points of the face, and that abstract is what the system actually uses. (While the defense has none of the validation studies of FIS, it can be reasonably

[1] Available at: http://www.perpetuallineup.org/

[2] Available at: http://www.nydailynews.com/new-york/nyc-crime/nypd-ripped-abusing-facial-recognition-tool-article-1.3847796

inferred that the lower the quality of the photo, the less reliable the abstract produced by FIS will be.) FIS runs the abstract through software that uses an algorithm to identify look-a-like photos (if any appear in the system). A "Facial Recognition Examiner" who is a trained NYPD technician, compares the look-a-like photographs to the probe photograph and determines whether any of them is a "match."

10. Many of the known facial-recognition programs, including the NYPD's[3] operate this way. They produce multiple look-a-like candidates (as opposed to a single "match"),[4] and a likelihood ratio for each look-a-like photograph.
11. Here, it is a near certainty that [redacted] photograph was one of several look-a-likes identified by the FIS software; and that each look-a-like had a confidence score of some type.
12. After FIS software identified a set of look-a-likes, a technician reviewing all look-a-like photos determined that [redacted] photo "matched" the probe photo.
13. An NYPD officer texted [redacted] mug shot to the LPO and asked "is this the guy [redacted]" The LPO responded "that's the guy." ***See* Exhibit 2** *(screen shot of the text messages).*[5]

[3] *See* Pei-Sze Chang, *Use of Facial Recognition Technology Expands as Some Question Whether Rules Are Keeping Up*, New York 4 , *available at* https://www.nbcnewyork.com/news/local/Facial-Recognition-NYPD-Technology-Video-Camera-Police-Arrest-Surveillance-309359581.html ("'We take images from unknown suspects supplied to us by detectives and we run the images through a facial recognition software,' said NYPD Sgt. Edwin Coello of the department's facial identification unit. 'That can give us back a list of several hundred candidates..'").

[4] *See* Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology* (Feb 12, 2018), available at https://www.eff.org/wp/law-enforcement-use-face-recognition#_idTextAnchor003.

[5] Based on information gleaned through the defense investigation (including interviews) the assertion by the police that the LPO had seen the sock thief "many times before" is a serious mischaracterization.

14. No police officer was present during the text message identification procedure. Thus, no law enforcement witness has firsthand knowledge of the circumstances under which the identification was made.
15. The LPO has had continuous possession of the photo since it was texted to him. No law enforcement officer can say can say how many times the LPO has looked at the photo, or for how long.
16. No live lineup or photo pack was ever conducted. The single photograph produced by the FIS and then identified via text message is the sole basis for probable cause to arrest.

[redacted]

DATED: [redacted]

_____

Kaitlin Jackson, Esq.

[redacted]

SUPREME COURT OF THE STATE OF NEW YORK
[redacted]

THE PEOPLE OF THE STATE OF NEW YORK

-against- MEMORANDUM OF LAW

[redacted] Ind. No. [redacted]

Defendant

INTRODUCTION

The defense seeks to (1) suppress identification testimony (or alternatively for a *Wade* hearing and a *Frye-Type* hearing on the reliability of FIS) and demands (2) discovery related to FIS, including *Brady* material related to FIS.

It is undisputed that showing a single photograph to a witness is suggestive. *See e.g. People v. Richards*, 36 N.Y.S.3d 49 (Rockland Cty. Ct. 2016). The defense moves to suppress all identifications of [redacted] as unnecessarily suggestive; or alternatively for a *Wade* hearing. *United States v. Wade*, 388 U.S. 218 (1967) and *Dunaway v. New York*, 442 U.S. 200 (1979).

In addition we are requesting that the court **suppress all identifications of** [redacted] **because the use of FIS rendered the risk of misidentification unacceptably high**; or alternatively for a hearing to determine the reliability of FIS. If the Government intends to offer evidence about the facial recognition match at trial, then [redacted] is entitled to a traditional *Frye* hearing. *Frye v. U.S.*, 293 F. 1013 (D.C. Cir. 1923). If the Government does not intend to introduce evidence about FIS, the court should still hold a hearing. FIS is an advanced technology that is designed to produce a slate of look-a-likes, people who look very much like

the person in a probe photo. There is a real risk that stranger eyewitnesses will conflate the person they saw and look-a-likes produced by FIS. This court should ensure that FIS is not increasing the likelihood of a misidentification, by requiring the Government to demonstrate that FIS "matches" are reliable during a *Frye-Type* hearing. If the Court determines that FIS does not meet the standards of scientific reliability laid out in *Frye*, then—the court should preclude any identification of a suspect produced by FIS because the risk of misidentification is unacceptably high.

Lastly, we demand information about how FIS operates, and copies of the other look-a-like photos that were selected in this case. The evidence in this case is so deeply wrapped up in the NYPD's facial recognition technology that we cannot provide a constitutionally effective defense without understanding how the purported match came to be.

MOTION TO SUPPRESS IDENTIFICATION TESTIMONY

I. *Single Photo Identifications are Presumptively Suggestive, and this Court Should Suppress Identification Testimony or Order a Wade/Rodriguez Hearing.*

It is undisputed that showing a single photograph to a witness is suggestive. *See* e.g., People v. Richards, 36 N.Y.S.3d 49 (Rockland Cty. Ct. 2016). [redacted] the Government served notice under C.P.L. § 710.30(1)(b) of their intent to introduce testimony regarding a police single photo identification of [redacted]. He moves to suppress this testimony on the following grounds:

1. The identification is not reliable because it is the product of an unnecessarily suggestive single photo identification procedure. *See United States v. Wade,* 388 U.S. 218 (1967).
2. The identification is the tainted fruit of an unlawful arrest. [redacted] was arrested based solely on a presumptively suggestive single photo identification procedure done over text message. He denies adamantly that he is the sock thief shown in the blurry surveillance, and the single identification made after an unusually suggestive procedure did not provide the police with probable cause to arrest him. Thus the identification must be suppressed as fruit of her unlawful arrest. See *United States v. Crews*, 445 U.S. 463 (1980).

If suppression is denied, [redacted] requests a *Wade/Crews* hearing. If the Government suggests that the identifying witness knew [redacted] "so well as to be impervious to police suggestion[,]" the defendant moves for a *Rodriguez* hearing. *See People v. Rodriguez*, 79 N.Y.2d 445, 452 (1992).] When the court finds that the single photo identification is suggestive,

the defense moves for an *independent source hearing* to challenge the admission of any in court identification testimony.

II. *The Use of FIS Unacceptably Increased the Chance of Misidentification, and this Court Should Suppress Identification Testimony or Order a Reliability Hearing.*

This court should hold a reliability hearing to determine whether FIS unacceptably increased the risk that [redacted] was misidentified. As the US Supreme Court explained in *Manson v. Braithwaite*, "reliability is the linchpin in determining the admissibility of identification testimony." *Manson v. Brathwaite*, 432 U.S. 98, 114 (1977). The *Wade* court shared the same sentiment ten years prior, explaining the dangers inherent in unreliable identification procedures:

> 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.' Wall, Eye-Witness Identification in Criminal Cases 26.

388 U.S. 218, 228–29 (U.S. 1967). New York State Courts have shared the same concern, opining that, "the vagaries of eyewitness identification have long been a concern of this court which has on occasion gone further than the Federal Constitution requires in order to further minimize the risk of mistaken identification." *People v. Hughes*, 59 N.Y.2d 523, 542 (1983).

The line of cases following *Wade, Braithwaite,* and their progeny are clear: **the Court's role in admissibility determinations for identification testimony, is limiting misidentifications.** In holding with that tradition, this court should order a hearing on the

scientific reliability of the NYPD's facial recognition software, because its use in this case may have unacceptably increased the chance of misidentification. FIS is new, untested by the courts, and not accepted in the scientific community.

Facial recognition systems are known to be prone to error. Even the FBI system only guarantees that "the candidate will be returned in the top 50 candidates 85 percent of the time *when the true candidate exists in the gallery*."[6] Here, the error rate of the FIS system is unknown, and there is no guarantee that a photograph of the actual sock thief is in the database. What is known, however, is that African-Americans are more likely to be misidentified by these systems than white people are.[7] Even makers of facial recognition systems have concluded that "existing software has not been exposed to enough images of people of color to be confidently relied upon to identify them."[8]

For context, it's worth noting that it is a current online fad to use facial recognition software "that matches people's selfies to famous works of art and encourages users to share the side-by-sides on social media …The latest version of the Google Arts & Culture app allows users to match their selfies against celebrated portraits pulled from more than 1,200 museums in more than 70 countries. The find-your-art-look alike feature has…has rocketed to viral status as more users shared their matches on Facebook, Twitter and Instagram… in a mix of implausible, absurd and "spot-on" comparisons."[9] **If look-a-likes can be found frequently in this limited dataset of famous works, it begs the question of how many look-a-likes we each have**. It

---

[6] *See* Lynch, *Face-Off supra* note X at 16 (internal quotation marks omitted, emphasis added).
[7] *Id.* at 9-10.
[8] Brian Bracken, *Facial Recognition Software Is Not Ready For Use By Law Enforcement*, Tech Crunch (June 25, 2018), available at https://techcrunch.com/2018/06/25/facial-recognition-software-is-not-ready-for-use-by-law-enforcement/.
[9] Hamza Shaban, *A Google app that matches your face to artwork is wildly popular. It's also raising privacy concerns., available at https://www.washingtonpost.com/news/the-switch/wp/2018/01/16/google-app-that-matches-your-face-to-artwork-is-wildly-popular-its-also-raising-privacy-concerns/?noredirect=on&utm_term=.68c30ccdacdb*

also begs the question of how easily facial recognition software can be fooled. It is possible (though maybe implausible) that the NYPD has access to better facial recognition technology than Google does. If that's the case, this Court should require the Government to present evidence to that effect at a hearing.

In New York, the reliability of a new scientific technology is typically tested during a *Frye* hearing. A *Frye* hearing in the traditional sense is probably not useful in this case. At the conclusion of a Frye hearing, the court makes a determination about the admissibility of expert testimony relating to the new scientific technique. *See* Frye v. U.S., 293 F. 1013 (D.C. Cir. 1923). Based on our review of other FIS cases, we've learned that the State has generally used FIS technology in a way that shields it from the Court's review. It has not been the practice of the State to put on expert testimony about FIS. As such, traditional Frye hearings have not been warranted.

Because this technology has significant reliability concerns, and because of the profoundly contaminating effect it could have had on the state's other evidence, it cannot be exempted from this Court's scrutiny. If the State **does** intend to introduce expert testimony we demand a traditional *Frye* hearing. But even if the State **does not** seek to admit expert testimony, Mr. [redacted] is **still** entitled to a *Frye*-type reliability hearing. At that hearing the court would hear evidence about the reliability of FIS, and make a determination as to whether the use of FIS *unreasonably increased the likelihood of misidentification* by the eyewitness in this case. If the Court finds that it did, then the remedy we seek is preclusion of identification testimony from the tainted witness.

This forensic technique requires a novel approach—lest it indefinitely evade judicial review. And judicial review of this technique is critical. The LPO relied on the FIS

"match" in making his identification, both because it was presented as a single photo, and because the knowledge that facial recognition selected [redacted] almost certainly artificially inflated the LPO's confidence in his identification. If the FIS "match" was not scientifically reliable, but produced an array of look-a-likes anyway, then the danger of misidentification is high in this case. That is particularly true, because there is no other evidence to suggest that [redacted] was involved in this sock theft.

While FIS is still a brand new technology, the Court of Appeals has made clear that eyewitness identifications contaminated by bad scientific practice are inadmissible. In particular, in *People v. Hughes* the Court prohibited an in-court eyewitness identification (and other testimony) when that testimony was influenced by an unreliable forensic practice. 59 N.Y.2d 523 (1983). The *Hughes* court held a *Frye-Type* hearing to address whether the "hypnotic[ly refreshed eyewitness testimony was] impermissibly suggestive under the totality of the circumstances." 59 N.Y.2d 523, 531–32 (1983). The trial court allowed the hypnotically refreshed testimony, but "the Appellate Division reversed in an opinion in which a majority of the court found that the trial court's decision "runs counter to the thrust of recent holdings in other jurisdictions that such evidence should not be permitted" unless it satisfies the criterion for the admission of scientific proof." 59 N.Y.2d 523, 532 (1983). The Court of Appeals affirmed.

In *Hughes* a rape victim was unable to identify her attacker. The police brought in a hypnotist to refresh her memory. At that point she identified the defendant. The *Hughes Court* held that the danger of unreliability in this circumstance was unacceptably high, explaining:

> The basic problem with admitting hypnotically generated statements or recollections in evidence is that hypnosis is an inherently suggestive procedure… [T]he hypnotic subject will be affected to some degree in three primary respects. First, a person who has been hypnotized becomes increasingly susceptible to

> suggestions consciously or unconsciously planted by the hypnotist or others present during the session…Second, the subject himself may confabulate, that is imagine incidents to fill memory gaps, by for instance imagining that he has experienced something he has simply heard from others… Third, a person who has recalled an incident under hypnosis will experience an increased confidence in his subsequent recollection of that incident.

People v. Hughes, 59 N.Y.2d 523, 534–35 (Ct. of App.1983). The Court explained that hypnosis has an appropriate place as an investigative tool, and that in some cases it might lead to other separately admissible evidence. However, when statements that are the direct product of hypnosis are introduced, the unreliability of this forensic technique becomes dangerous:

> Scientific experts have no general objection to the investigative use of hypnosis provided the posthypnotic recollections are used only as leads to other evidence which then serves to solve or prove the crime. The potential unreliability of the hypnotic statements will be resolved or rendered moot as soon as the lead has been investigated. But the side effects of hypnosis cannot be so easily discounted if the hypnotically induced statements are later sought to be introduced at trial.

People v. Hughes, 59 N.Y.2d 523, 536 (Ct. of App. 1983). The witness was allowed to testify about statements she made prior to the hypnosis, but all post hypnosis statements, including *any identification* were prohibited.

The *Hughes* Court rejected the Government's argument that unreliable forensics used to obtain identifications only pose an admissibility issue when the Government seeks to introduce expert testimony. The *Hughes* court explained:

> The prosecutor urges…that the testimony will come from a lay witness and not an expert claiming scientific endorsement for the procedure employed. This, he contends, should eliminate the primary difficulty with scientific proof, namely that the jury or fact finder may be unduly impressed with the scientific and presumably reliable basis for the evidence presented…Although he recognizes that the use of hypnosis to refresh recollection is relatively new and unusual he urges that it is no worse than the other methods currently accepted in the law.
>
> In essence then the prosecutor urges that we…give a more restricted reading to the rule governing the admissibility of scientific proof. However, the current trend of the law, when dealing with suggestive or scientific procedures relating to

> eyewitness testimony, particularly in this State has been to take the opposite course.

59 N.Y.2d 523, 541 (1983). This court should take up the *Hughes* court's charge and require the Government to demonstrate that the forensic technique used to obtain the identification is reliable—regardless of whether the Government seeks to introduce expert testimony. The *Hughes* court explained that it is incumbent on trial courts to ensure that identifications are not the product of unreliable forensics, opining:

> When presented with scientific evidence purporting to gauge the credibility of participants or witnesses to a criminal incident, we have established a very high level of reliability, tantamount to certainty, as a predicate for its admissibility. Although ordinary scientific proof need not meet such a demanding standard, the increased certitude has been found appropriate when the fallibility of the scientific procedure might directly affect the fact finder's assessment of eyewitness credibility.

59 N.Y.2d 523, 542 (1983).

FIS is a different type of forensics than hypnosis, but the problem takes the same shape. Facial recognition may be a useful tool for finding leads and discovering separately admissible evidence. But **when the State seeks to introduce identifications that are simply confirmations of what FIS has already determined, the scientific reliability of FIS becomes an issue.** Many of the same concerns that the *Hughes* Court addressed are at play here. The LPO relied on the FIS "match" in making his identification, both because it was presented as a single photo, and because the knowledge that facial recognition selected [redacted] almost certainly artificially inflated the LPO's confidence in his identification. Additionally, strangers are unlikely to be able to distinguish between a person they saw, and a look-a-like. Thus, it's critical that this court hear evidence and make a determination about whether FIS makes reliable selections.

A King's County Court citing *Hughes* addressed the explicit question of whether trial courts have the power to hold novel types of admissibility hearings. *People v. Michael M.*, 162 Misc. 2d 803, 806 (BK Sup. Ct. 1994). In *Michael M.* the defense requested a suppression hearing on whether or not suggestive questioning of a child witness by a civilian (in a rape case) rendered the child's testimony unreliable and inadmissible. The *Michael M. Court* opined that "[s]ince suggestive questioning of a witness by a civilian physician is not a ground for suppression listed in CPL article 710, defendant's hearing request is not specifically authorized by the CPL." (Note that this particular problem does not present itself in this case, as suppression hearings for identifications are authorized by CPL 710.). However, the Court found that part of the essential functioning of a trial court is holding admissibility hearings on evidentiary matters—even when the issues are novel. The *Michael M.* Court explained:

> A court's power to admit or exclude evidence under the rules of evidence is inherent in its power to function as a court…Courts have recognized the right of a trial court to determine evidentiary matters at pretrial hearings, despite the lack of specific authorization in the CPL. The court finds that it has the inherent power to entertain defendant's motion, despite the lack of specific statutory authority.

People v. Michael M., 162 Misc. 2d 803, 806–07 (BK Sup. Ct. 1994) *(internal citations omitted).*

The hearing we are requesting is significantly less novel than the hearing sought in *Michael M.*—suppression hearings regarding identification testimony are specifically contemplated by CPL 710 and are common. *Frye* already provides a roadmap for the hearing, even though the remedy we seek is different. It is critical that this Court order a *Frye-Type* hearing to determine whether the way FIS was used in this case rendered the identification unreliable.

DEMAND FOR DISCOVERY RELATED TO FIS

[redacted] cannot mount a defense without an understanding of why he was selected by FIS. Consequently, the Government must produce discovery related to the use of FIS. C.P.L. § 240.20(1)(c) lays out the government's disclosure obligations with regards to scientific (and forensic) evidence:

> Any written report or document, or portion thereof, concerning…scientific test or experiment, relating to the criminal action or proceeding which was made by, or at the request or direction of a public servant engaged in law enforcement activity…

The use of facial recognition software to identify defendants (and/or their look-a-likes) falls squarely within this provision. Law enforcement officers enter photos into a software program that uses complex algorithms to quickly compare facial features across tens or hundreds of thousands of photographs. This process necessarily includes official procedures, error rates, algorithms, etc., the disclosure of which is vital to the defense in this case.

This is an issue of first impression. The defense was able to find only one case where a New York court considered a discovery request related to FIS —an unpublished decision out of Brooklyn (**See Exhibit 3**- *New York vs. Junior Roland*). That opinion provides little guidance, because the facts are so dissimilar. In *Roland* the defendant was charged with two separate robberies. The complainant from one of the robberies found a photo of the defendant on social media and provided it to the police. The police put the photo through FIS. FIS matched the photo (provided by the complainant) to Mr. Roland. The police then put Mr. Roland in a live lineup procedure for the complainant from the other robbery. That complainant also positively identified the defendant. The *Roland* defendant also made an inculpatory statement.

The *Roland Court* held that the government did not have to produce discovery about the use of FIS, opining:

> Here, with respect to the specific facts of this case, this court finds that the police utilized the Facial Recognition software as an investigative tool to confirm the identification initiated by [complainant 1]. In fact, the photos Detective Maynard submitted to the FIS were provided by [complainant 1]. Further, the People do not claim that the confirmatory identification procedure conducted with this complainant established probable cause for the arrest of the defendant. After the confirmatory photographic identification of the defendant, Detective Maynard issued an I-Card for the defendant. Thereafter, defendant was placed in a lineup and identified as the perpetrator by [complainant 2].

In *Roland*, FIS played a very different role than it did in this case. In *Roland*, the first identification was totally unrelated to FIS, and the second had only an attenuated connection to it. The second complaint picked the defendant out of a live lineup. FIS was used simply to get more information about the defendant, who had already been identified. There was no reason to believe that the use of FIS had a significant impact on the trajectory of the case or on the complainants. Additionally, though the court didn't address it, it' is noteworthy that there was incriminating evidence totally separate from FIS, importantly a statement from the defendant.

The same is not true in [redacted] case. FIS is the whole case—there is no evidence unrelated to FIS for the government to use. And there aren't the same markers of reliability in the identifications that rendered the police's use of FIS "merely investigative" in Roland. Unlike in Roland, FIS made the initial "identification" of [redacted], and the LPO simply confirmed the choice FIS had already made. A fair identification was never held to ensure that FIS had selected the right person.

This court should order discovery. We cannot put forth a constitutionally effective defense without understanding how FIS selected [redacted] photograph.

The defense demands the following items of discovery:

1. CANDIDATE LIST:

a. The candidate list generated from the Facial Identification Section software and examined by Detective [redacted].

    i. Any electronically generated information related to the candidate list generated from the Facial Identification Section software and examined by Detective [redacted], including but not limited to, the defendant's location or ranking within the candidate list and the similarity or confidence level score associated with each candidate, including the defendant.

    ii. Any notes/communications/writings by Detective [redacted] regarding the selection of [redacted] photo from the candidate list.

2. PHOTOS:

    a. The original color digital copy of the screenshot probe photograph submitted to FIS that returned a match, and information indicating the image quality.

        i. All edited copies of the probe photograph submitted.

    b. The original color digital copy of the arrest photograph of the defendant that is enrolled in the Facial Identification Section database and information indicating the image quality.

        i. All edited copies of the arrest photo that are in the database.

    c. Copies of other photo screenshots taken from the surveillance video and submitted to FIS, whether or not the returned a match result.

        i. All edited copies of other screenshots that were entered in the database.

3. SOFTWARE:

    a. Name and manufacturer of the FIS software used in this case, as we well as the algorithm(s), version number(s) and year(s) developed.

    b. Documents describing the intended theory and process for the probabilistic model used by the FIS software.

    c. Source code for the FIS software and face recognition algorithim(s).

        i. Performance of the algorithim(s) on applicable NIST Face Recognition tests, if available.

    d. What measurements, nodal points, or other unique identifying marks are used by the system in creating facial feature vectors. If weighted differently, what are the scores given to each respective mark.

e. Error rates for FIS, include false accept and false reject rates (also called false match and false non match rates—FMR and FNMR).

    i. Documentation of how the error rates were calculated, including whether they reflect test or operational conditions.

f. A copy of the user manual for the FIS version in use for this case.

g. Any internal validation studies of the FIS software, including reports of errors or bugs.

h. All inputs and user or operated selected parameters for any FIS runs relevant to this case, including but not limited to any editing or modifications to the probe photo.

i. All electronic data files produced by the FIS software and/or its operated for all runs relevant to this case.

j. The results of any proficiency testing for the FIS operator.

k. The results of any calibration, proficiency tests, or performance checks for the FIS system.

l. Any communications logs or records relating to the FIS analysis in this case, including any bug/crash reports, corrective actions, software updates, or any other relevant records.

4. DATABASE:

a. Documents relating to the number of in the database and how those photos are obtained.

    i. Including, but not limited to any documents referencing how [redacted] photo came to be in the database.

b. Any documents about how often photos are removed from the database as well as the process for getting photos removed.

c. Documentation about who has access to the database, as well as all documentation about the privacy policy for the database.

d. All written instructions for maintaining the database.

e. All documents referencing training datasets used in the creation of the FIS modeling system, including the distribution by race and ethnicity; sex; and age in the training datasets.

5. OTHER:

a. Any other reports generated by the Facial Identification Section database in relation to the inquiry into the probe photograph.

b. Notes made by the analyst using FIS.

The name, training and qualifications of the analyst who ran the FIS inquiry.

BRADY DEMAND

[redacted] was not the only look-a-like selected by the FIS software. He is seeking information related to the other candidates selected by the software. The defense demands disclosure of all material favorable to the defense pursuant to the constitutions of the United States and New York, and under *Brady, Giglio, Kyles* and their progeny. C.P.L.§ 240.20(1)(h). This includes not only material that is exculpatory or mitigating, but also material related to **impeachment of state's witnesses**. Additionally, this request includes all information known to the government that is favorable to the defense, whether or not it is admissible in court.

The material we demanded is a small part of what we demanded in the discovery demand in the previous section. **The pieces of discovery that we believe we are entitled to under *Brady*, are**:

1. The candidate list generated from the Facial Identification Section software and examined by Detective [redacted]
2. The defendant's location or ranking within the candidate list and the similarity or confidence level score associated with each candidate, including the defendant.
3. Any notes/communications/writings by Detective [redacted] regarding the selection of [redacted] photo from the candidate list.
4. Any electronically generated information related to the candidate list generated from the Facial Identification Section software and examined by Detective [redacted]

[redacted]

[redacted]

[redacted]