IN THE FLORIDA SUPREME COURT

No. SC2019-0298

WILLIE ALLEN LYNCH,
Petitioner,

v.

STATE OF FLORIDA
Respondent.

Appeal from Florida First District Court of Appeal
No. 1D16-3290

AMICI CURIAE BRIEF OF AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF FLORIDA, ELECTRONIC FRONTIER FOUNDATION, GEORGETOWN LAW'S CENTER ON PRIVACY & TECHNOLOGY, AND INNOCENCE PROJECT IN SUPPORT OF PETITIONER

Benjamin James Stevenson
Fla. Bar. No. 598909
ACLU Found. of Fla.
3 W. Garden St., Suite 712
Pensacola, FL 32502-5636
T. 786.363.2738
bstevenson@aclufl.org

Counsel for Amici Curiae

Jennifer Lynch
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
T. 415.436.9333
jlynch@eff.org

Clare Garvie
Alvaro M. Bedoya
Center on Privacy & Technology
Georgetown University Law Center
600 New Jersey Ave NW
Washington, D.C. 20001
T. 202.661.6707
cag104@law.georgetown.edu

Alexis Agathocleous
Innocence Project, Inc.
40 Worth Street, Ste. 701
New York, New York 10013
T. 212.364.5968
agathocleous@innocenceproject.org

Vera Eidelman
Nate Wessler
Andrea Woods
Brandon Buskey
Brett Max Kaufman
Rachel Goodman
ACLU Foundation
125 Broad Street, 18th Fl.
New York, NY 10004
T. 212.549.2500
veidelman@aclu.org

Somil Trivedi
ACLU Foundation
915 15th Street, NW
Washington, DC 20005
T. 202.715.0802
strivedi@aclu.org

Of Counsel

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF *AMICI CURIAE*

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with more than two million members dedicated to defending the civil liberties guaranteed by the Constitution. The ACLU of Florida is a state affiliate of the ACLU. The ACLU and the ACLU of Florida have appeared in numerous cases, both as direct counsel and as *amici*, before courts in Florida and throughout the nation in cases involving the meaning and scope of the rights of criminal defendants and the legal limitations on the use of technology by police and prosecutors.

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for nearly 30 years. With roughly 40,000 active donors, EFF represents technology users' interests in court cases and broader policy debates. EFF regularly participates as *amicus* in federal and state courts, including in the United States Supreme Court, in cases addressing the impact of novel technologies on criminal investigations and the justice system. *See, e.g.*, *Carpenter v. United States,* 137 S. Ct. 2211 (2017); *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015), *Riley v. California*, 573 U.S. 373 (2014); *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015).

Georgetown Law's Center on Privacy & Technology is a think tank whose work focuses on the impacts of government surveillance and commercial data practices on vulnerable communities. The Center researches and advocates for reforms to state and federal consumer and government privacy laws, particularly for new technologies such as face recognition, as in its 2016 report *The Perpetual Line-Up*, www.perpetuallineup.org. Its staff provides education and technical assistance to legislators, attorneys, and the public on emerging technologies and their impacts on privacy, civil liberties, and civil rights.

The Innocence Project, Inc. ("Innocence Project") is a non-profit organization dedicated to providing pro bono legal and related investigative services to indigent prisoners whose actual innocence may be established through post-conviction DNA evidence. The Innocence Project also seeks to prevent future wrongful convictions by researching their causes and pursuing legal, legislative and administrative reform initiatives designed to enhance the truth-seeking functions of the criminal justice system. To date, the work of the Innocence Project and affiliated organizations has led to the exoneration of 364 individuals by post-conviction DNA testing. The Innocence Project is committed to ensuring, as an essential component of a fair and just determination of the facts, that judicial decisions are premised upon sound investigative practices by law enforcement agencies and the application of proven scientific methodology in criminal cases.

SUMMARY OF ARGUMENT

Defendant Willie Lynch was sentenced to eight years in prison after the police implicated him using an unproven, error-prone face recognition algorithm. The case turned on identity: Mr. Lynch argued that the state had misidentified him, while the state relied on the algorithm as the cornerstone of its investigation.

The state built its case from the algorithm's results even though: how the algorithm functioned was a mystery to the crime analyst who operated it and the detective who accepted its conclusion (Sec Supp R I 11, 27); the Assistant State Attorney doubted the system was reliable enough to meet the evidentiary standard for use at trial (R II 380); the defense did not learn of the algorithm's use in this case until eight days before the final pretrial hearing; and the prosecution never disclosed crucial information about the system to the defense, including the other photographs it identified as potential matches.

Understanding how facial recognition functions and how it was used here is critical to understanding why this case merits review. Face recognition algorithms, including the one used in this case, are prone to error. Yet, Florida uses the face recognition system at issue here tens of thousands of times a year to attempt to identify individuals. Despite demonstrated flaws in the technology, the State appears to consistently fail to produce information about its use to people accused of crimes. This Court should exercise jurisdiction to address the questions of great

public importance raised by this case, and to provide guidance to the more than 240 law enforcement agencies across Florida who use this technology.

This Court should also exercise jurisdiction to correct the First District's erroneous due process holding. Had a witness who identified Mr. Lynch stated that other individuals in a line-up also looked like the perpetrator, the State would have had to disclose that information, as well as any information indicating that the witness was uncertain or impaired when making the identification. Here, those same principles should have required the State to disclose the other photos the algorithm identified as potential matches and information about how the algorithm functions.

BACKGROUND

In September 2015, an undercover detective snapped several photos of a suspect using his cell phone's camera. (R II 302). He did not use a modern smart phone, but rather "an old Tracfone from Wal-Mart." (R II 312). Because he was trying to be discrete, the detective took the photos while holding the phone to his ear and pretending to be on a call, as the suspect "was walking out of the apartment building and approaching [him]." (R II 302). As a result, the photos depict the suspect from an oblique angle, off-axis, and are blurred in places. (R I 141–146).

Because neither of the involved officers recognized the suspect (they knew only that he was a Black male who called himself "Midnight") (R II 300–01, 341),

they sent the photos to a Jacksonville Sheriff's Office crime analyst for assistance. (Sec Supp R I 21). The analyst ran one of the photos through a face recognition algorithm to see if it was similar to any county booking photos. (*Id. at* 8–12). The program returned several possible matches, but it did not express more than "one star" of confidence in any match being correct.[1] (*Id.* at 11–12). The Defendant's booking photo from a previous arrest was listed first among the results. As the analyst explained, however, the first-listed photo is not necessarily the best match; sometimes a result further down in the list is the best one. (*Id.* at 11). After reviewing the photos, the analyst sent only the first result—the Defendant's mug shot—and his entire criminal history, to the officers for their review. (*Id.* at 10, 21).

The face recognition algorithm used here is part of the Face Analysis Comparison Examination System (FACES), a program the Pinellas County Sheriff's Office operates and makes available to law enforcement agencies throughout the state. (*Id.* at 12).[2] The algorithm operates in two basic steps.[3] First, it processes the image an analyst is seeking to match (often called a "probe image"). This often involves "pose correction" and "face normalization," which

---

[1] The analyst did not know what number of stars is possible. (Sec Supp R I 10–12).
[2] *See also* Benjamin Conarck, *How an Accused Drug Dealer Revealed JSO's Facial Recognition Network*, Florida Times-Union (Nov. 11, 2016), https://bit.ly/2H5wMxT.
[3] *See FACES Training 2015*, 014383–04417, at 5, Pinellas County Sheriff's Office, https://drive.google.com/drive/folders/0B-MxWJP0ZmePQ2kyMm1LVFVnOTg.

rotates the image to match the pose of the photos to be matched and approximates what any missing parts of the face look like.[4] The system also generates a "faceprint,"[5] often by "extract[ing] features . . . like eye position or skin texture."[6] Second, the algorithm compares the faceprint of the probe image to faceprints of images in the database and returns several potential matches, which it generally presents in order of the algorithm's confidence in the match.[7] (*See also* Sec Supp R I 11). By comparing a probe image to photos in a database of known persons, the algorithm can attempt to find matches to the person depicted in the probe.

Face recognition systems like FACES are probabilistic, meaning they do not "produce binary 'yes' or 'no' answers, but rather identif[y] more likely or less likely matches." Thus, "[m]ost police face recognition systems will output either

---

[4] The probe taken of Mr. Lynch has him slightly turned from the camera; face normalization will rotate that image to a pose facing the camera and add in an approximation of what the hidden part of the face looks like.

[5] U.S. Gov't Accountability Off., GAO-15-621, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law* 3 (2015), https://www.gao.gov/assets/680/671764.pdf. "A faceprint . . . is essentially a digital code that a facial recognition algorithm creates from an image." *Id.* at 3 n.5.

[6] Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America* 9, Georgetown Law Center on Privacy & Technology (2016), https://www.perpetuallineup.org/.

[7] This is distinct from the probability that the two photos are, in fact, matches, and inherently expresses uncertainty in the match. *See* Nicole A. Spaun, *Face Recognition in Forensic Science*, *in* Handbook of Face Recognition 667, Stan Z. Li & Anil Jain, eds. (2011). It is akin to a witness saying "I am X% certain that he's the same guy," rather than "it is X% likely that he is the perpetrator."

the top few most similar photos or all photos above a certain similarity threshold."[8] Along these lines, the FACES algorithm does not purport to provide a definitive match, but rather "returns an image gallery of rank-ordered results for review."[9]

Like all computerized algorithms, face recognition algorithms are not neutral, infallible truth tellers. Face recognition systems "vary in their ability to identify people, and no system is 100 percent accurate under all conditions."[10] As the crime analyst noted in this case, with FACES, "the [best] photo [match] may not [be] the first or the second" returned by the program. (Sec Supp R I 11).

The accuracy of face recognition is directly affected by the quality of the photos being searched—error rates will be greater when two photographs contain different lighting, shadows, backgrounds, poses, or expressions.[11] Face recognition can be extremely poor at identifying a person in a low resolution image[12] or a

---

[8] *Perpetual Line-Up*, at 9.

[9] *FACES Training 2015*, at 5; *see also* (Sec Supp R I 11 (discussing "the several photos that the software returned")).

[10] Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology* 6, Electronic Frontier Foundation (2018) https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf.

[11] *See, e.g.,* P. Jonathon Phillips, et al., *An Introduction to the Good, the Bad, & the Ugly Face Recognition: Challenge Problem* 346, Nat'l Inst. of Standards & Testing (Dec. 2011), www.nist.gov/itl/iad/ig/upload/05771424.pdf (noting only 15 percent accuracy for face image pairs that are "difficult to match").

[12] *See, e.g.,* Min-Chun Yang, et al., *Recognition at a Long Distance: Very Low Resolution Face Recognition and Hallucination*, IEEE 2015 Int'l Conf. on Biometrics, 237–42 (2015).

video,[13] or at accurately finding matches when searching against a large database of images, in part because so many people within a given population look similar to one another.[14] This case exemplifies many of these problems: the suspect was photographed using an older-model cell phone, at an oblique angle, in uneven lighting conditions, while he was in motion. All these are variables that will serve to lower the overall accuracy of the subsequent face recognition search.

Such errors—and the high rates of false positives and false negatives that accompany them[15]—are exacerbated when the algorithms are used on photos of certain demographic groups, including Black people like the Defendant here. Face recognition systems' accuracy rates are closely tied to the data—or faces—used to train them.[16] Systems "learn" how to identify faces by analyzing previously identified images in a training dataset. If the images in the dataset do not represent the population of people the system is ultimately used to identify, then accuracy

---

[13] *See generally*, Nat'l Inst. Of Standards & Testing, *Face in Video Evaluation*, https://www.nist.gov/programs-projects/face-video-evaluation-five.

[14] *See, e.g.*, Adrienne LaFrance, *The Ultimate Facial-Recognition Algorithm*, Atlantic (June 28, 2016), https://bit.ly/2XJp811.

[15] A "false positive" occurs when the system identifies a match, but that match is incorrect. A "false negative" occurs when the system fails to make a match.

[16] *See* Brendan F. Klare, et al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE Transactions on Info. Forensics and Sec. 6, 1789–1801 (Dec. 2012), https://bit.ly/2TGiWaO; Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research (2018), https://bit.ly/2Ek9ZwZ.

rates drop significantly. This is a problem for many of the face recognition algorithms in use today. Their training "datasets typically feature celebrities," which "makes it easier to label thousands of individual faces, but fails to capture the full range of human diversity."[17] A recent MIT study found two datasets used to train face recognition algorithms were "overwhelmingly composed of lighter-skinned subjects."[18] Additional sources of bias are introduced when face recognition systems rely on digital camera images because, when taking photos of darker-skinned faces, the cameras fail to provide the degree of color contrast that the algorithms need to produce and match faceprints.[19]

A number of researchers, including a Senior Level Photographic Technologist for the FBI, have reported that face recognition algorithms misidentify Black people, young people, and women at higher rates than white people, older people, and men, respectively.[20] In a recent test, when set to default settings, one face recognition algorithm being marketed to law enforcement agencies falsely matched photographs of 28 members of Congress with photos of arrestees from a mug shot database: While people of color made up approximately

[17] *Perpetual Line-up,* at 50–51.
[18] Buolamwini & Gebru, *supra* note16.
[19] *Perpetual Line-up,* at 54.
[20] *See, e.g.*, sources cited *supra* note 16.

20 percent of members of Congress generally, they constituted nearly 40 percent of the false matches returned by the algorithm.[21]

Even when, as in this case, a human reviews the algorithm's results, that review might fail to correct an inaccurate identification. Research conducted by the National Institute of Standards and Technology and others has shown that people are likely to believe computer-generated results, and that those who are not specially trained in face recognition are poor at identifying people they do not know,[22] even if they perform face identifications as part of their daily work.[23] And even trained facial specialists misidentify subjects about 10% of the time.[24]

The State recognized the manifold problems with face recognition technology in this case and acknowledged on the record that FACES was probably not reliable enough to meet the evidentiary standards for use at trial. (R II 380).

---

[21] Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU Free Future (July 26, 2018), https://bit.ly/2OkETHe.

[22] P. Jonathon Phillips et al., *Face Recognition Accuracy of Forensic Examiners, Superrecognizers, and Face Recognition Algorithms*, PNAS (2018), https://bit.ly/2VGgaji; David White, et al., *Error Rates in Users of Automatic Face Recognition Software*, Plos One (2015), https://bit.ly/2TlTpVl (noting participants made over 50% errors for adult target faces).

[23] White, et al., *Error Rates*, *supra* (finding equivalent performance between untrained examiners and passport officers).

[24] Phillips, *Face Recognition Accuracy*, *supra*.

In the context of police investigations, where misidentification can lead to deprivation of liberty, face-recognition technology is particularly dangerous, raising questions about whether it should ever be used by law enforcement. Without judicial oversight and robust adversarial testing of the reliability of decisions made based on these algorithms' results, the accuracy of investigations and convictions in Florida will be called into increasing doubt.

ARGUMENT

I. This case raises questions of great public importance.

Clarifying the rights of defendants to obtain information about the use of face recognition technology in their cases is an issue of "great public importance" that requires resolution by this court. *See* R. App. P. 9.030(a)(2)(A)(v).[25]

In this case, as in tens of thousands of investigations each year, Florida law enforcement agents used FACES to attempt to identify an individual. (Sec Supp R I 8–12). FACES, which was launched by the Pinellas County Sheriff's Office in 2001, is now used by more than 240 law enforcement agencies across Florida, with

[25] *Amici* acknowledge that Fla. Const. Art. 5, § 3(b)(4) grants this Court discretionary jurisdiction when the District Court of Appeals certifies a question to be of great public importance, but that no certification was made in this case. As explained below, *infra* Part II, *amici* agree with Petitioner that this Court has jurisdiction to review this decision because it "expressly and directly conflicts with a decision of another district court of appeal" and "expressly [mis]construes a provision of the . . . federal constitution." Fla. Const. Art. 5, § 3(b)(3). The great public importance of the issues in this case provides additional reason for review.

more than 5,000 users conducting up to 8,000 searches per month.[26] The system allows police to search over 33 million faces, including license and ID photos, and law enforcement photos like the booking photos searched in this case.[27]

Despite the heavy use of FACES in criminal investigations across the state, its operation is poorly regulated and shrouded in secrecy. The Pinellas County Sheriff reports that his office does not audit the system for misuse.[28] In Jacksonville, Sheriff's Office crime analysts run queries on the system despite the absence of a written policy governing its use, and despite the fact that the Office has not "been able to validate the system" and "cannot speak to the algorithms and the process by which a match is made."[29] *Amici* are not aware of any publicly available information about FACES' accuracy rates in operational conditions.

Because forensic algorithms like FACES combine many potential sources of error and bias—from the foundational assumptions underlying the algorithms, to the dataset humans choose for the machine to learn on, to the source code they write to operationalize it—forensic algorithms often fail to meet the needs of a rigorous and fair judicial system. For example, in just the last few years,

---

[26] *Perpetual Line-up*, at 25 and Appendix XIV, *available at* https://bit.ly/2XKSR9Z.
[27] *Id.*
[28] *Id.* at 60.
[29] Call Log, Notes from Jacksonville Sheriff's Department, Fla., Re: Request # REC9135, 010708–010709 (Feb. 17, 2016), https://drive.google.com/drive/folders/0B-MxWJP0ZmePNzZkRlAzVmpJZHc.

researchers have documented errors in algorithms used to test complex DNA samples that materially altered results in criminal trials.[30] Similarly, in a 2008 case, a defense expert's review of a breathalyzer's source code "documented 19,500 errors, nine of which he believed could ultimately affect the breath alcohol reading,"[31] and led the New Jersey Supreme Court in another case to require modifications to prevent misleadingly high readings. *State v. Chun*, 943 A.2d 114, 120–21 (N.J. 2008). Face recognition systems are similarly susceptible to error and to misrepresenting results as more certain than the science supports.

Despite the significant possibility of error and the enormous significance of incorrect or unreliable results, among the thousands of cases in which the state uses FACES each year, this appears to be the only reported case in Florida addressing use of the system. That suggests widespread failures to disclose information about use of FACES to defendants and courts. Indeed, the Pinellas County Public Defender reports that in the 15 years FACES has been operational, "his office has never received any face recognition information as part of a *Brady* disclosure."[32] In this case, the defense learned of the program's use a mere eight days before the

---

[30] Lauren Kirchner, *Traces of Crime: How New York's DNA Techniques Became Tainted*, N.Y. Times (Sept. 4, 2017), http://nyti.ms/2vJwxze; David Murray, *Queensland Authorities Confirm 'Miscode' Affects DNA Evidence in Criminal Cases*, Courier-Mail (Mar. 20, 2015), https://bit.ly/2Ht8IV5.

[31] Andrea Roth, *Machine Testimony*, 126 Yale L.J. 1972, 2025 (2017) (internal marks omitted).

[32] *Perpetual Line-up* at 59.

final pretrial conference. This case provides a critical opportunity for the Court to ensure the integrity of the criminal justice system in this state, by providing guidance on what information is due to defendants under *Brady* and related rules.

II. Exculpatory and impeachment information related to FACES is *Brady* material, just as such information from a human witness would be.

This Court also has jurisdiction to review this case because the First District's decision erroneously construes the Due Process Clause of the federal Constitution, as interpreted by *Brady* and its progeny. *See* Fla. Const. Art. 5, § 3(b)(3); Pet's Br. at 9–10. The First District failed to recognize the State's responsibility to disclose material information that tends to exculpate the defendant and/or undermine the credibility of its witnesses. *See Brady v. Maryland*, 373 U.S. 83 (1963); *Kyles v. Whitley*, 514 U.S. 419 (1995); *Floyd v. State*, 902 So.2d 775 (Fla. 2005); *see also Chambers v. Mississippi*, 410 U.S. 284, 294 (1973) (due process guarantees, "in essence, the right to a fair opportunity to defend against the State's accusations."). Information is material if it tends to undermine confidence in the result of the criminal case. *United States v. Bagley*, 473 U.S. 667, 682 (1985). The state must disclose such information whether or not the defense has requested it, *United States v. Agurs*, 427 U.S. 97, 110–11 (1976), and regardless of whether the State called the witness most closely related to that information to testify, *State v. Huggins*, 788 So.2d 238, 243 (Fla. 2001).

a. FACES is unreliable in many ways that human witnesses are, and Mr. Lynch should be able to test its unreliability in the same way.

The analyst's use of the FACES program to identify Mr. Lynch created information that would tend to exculpate him and/or impeach the state's witnesses, including but not limited to: (1) other possible matches FACES generated, indicating the possibility of alternate perpetrators; (2) the analyst's choice to send only Mr. Lynch's photo to investigators, indicating improper suggestiveness; (3) the range of possible star ratings; (4) an executable version of the software and the source code (which is prone to error and bias); and (5) the analyst's lack of training in forensic face analysis. All of this evidence would have indicated uncertainty in the identification procedure.

If any of this information had come from a human witness—or, in the case of the analyst's suggestive submission to the investigators, a lineup—it would clearly be *Brady* material. For example, FACES identified Mr. Lynch and several other people with similar confidence as the perpetrator. (Sec Supp R I 9–10). Had an eyewitness done so, the state would be unquestionably obligated to disclose the identification of the alternate suspects. *Floyd*, 902 So.2d at 781 ("the exculpatory nature of this evidence is apparent, since the interviews present direct evidence of two other persons who may have committed the crime"); *Rogers v. State*, 782 So.2d 373, 383 (Fla. 2001) (undisclosed police reports "could have been used to show that another person" committed the crime, "as is reflected by the many

witness descriptions" matching the alternate suspect). Therefore Mr. Lynch should have the opportunity to review the other possible matches, to both investigate those alternate leads and impeach the officers who identified him confidently.

The FACES program also expressed only a one-star confidence level in its identification of Mr. Lynch, indicating a lack of certainty, and even the analyst did not know how the program works or the maximum number of stars. (Sec Supp R I 10–12). Moreover, all computer programs built through source code contain glitches, but these defects are difficult to quantify or describe without scientific testing. *See, e.g.*, Christian Chessman, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 Cal. L. Rev. 179, 186 (2017) (even highly experienced programmers make a mistake in "almost 1% of all expressions" in source code). The risk of bugs only increases with the complexity of the code and the difficulty of the problem it is attempting to solve, Roth, *Machine Testimony*, 126 Yale L.J. at 2024, and face-matching is an exceedingly difficult task for an algorithm, *see* Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, *supra*.

If FACES were a human witness who expressed a low level of confidence in his or her eyewitness identification, or admitted to a mistake in that identification, those facts would be *Brady* material. *See Jacobs v. Singletary*, 952 F.2d 1282, 1288 (11th Cir. 1992) (undisclosed report revealing that witness was "uncertain"

and "unsure" about certain facts undermined his more confident later testimony and therefore constituted *Brady* material); *Conley v. U.S.*, 332 F. Supp. 2d 302, 316 (D. Mass. 2004), *aff'd*, 415 F.3d 183 (1st Cir. 2005) (undisclosed memo containing admission that witness was unsure of prior recollection was "critical information" and material under *Brady*).

Accordingly, Mr. Lynch should have the opportunity to review information about FACES including: the algorithm's underlying model; training data; source code; operating manual and other explanatory documentation; any other results from which the final, reported result was chosen; and any validation studies.[33] That information is necessary to understand, among other things, how uncertain a one-star rating is, what physical attribute-matches might have resulted in that rating, why the algorithm listed Mr. Lynch first, and why the analyst chose Mr. Lynch's photo over other photos returned as matches.[34]

Finally, FACES is an algorithmic program created, operated, and interpreted by humans, and all humans possess conscious and unconscious biases. In particular, state forensic scientists may possess biases in favor of their client, the

[33] In general, defendants should also have the opportunity to examine the individuals who used and created the system.

[34] *See, e.g*, Order on Procedural History and Case Status, *United States v. Michaud*, No. 3:15-cr-05351-RJB (W.D. Wash. May 18, 2016), ECF No. 205 (holding that source code underlying technique used to identify defendant was material and defendant therefore has a right to access it before the trial).

prosecution. *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 318 (2009) ("A forensic analyst . . . may feel pressure—or have an incentive—to alter the evidence in a manner favorable to the prosecution."). This bias is only likely to be exacerbated where, as here, the individuals operating, analyzing, and interpreting the results are aware of the identified individual's criminal history. *See* Itiel E. Dror & Greg Hampikian, *Subjectivity and Bias in Forensic DNA Mixture Interpretation*, 51 Sci. & Just. 204, 205–07 (2011) (finding that more forensic examiners determined that an individual matched a DNA mixture when they knew he was a defendant in a gang rape case than when they did not). Mr. Lynch should receive discovery sufficient to probe the biases and assumptions built in to FACES' selection of him as a possible match and to undermine the analyst's choice to forward only his information to the investigators in this case.

b. The State's use of FACES was akin to creating a one-person line-up, and the State has an obligation to disclose information related to its suggestiveness.

The analyst's decision to send only Mr. Lynch's mugshot, along with his entire criminal history, to the police officer witnesses in this case is the functional equivalent of showing an eyewitness a lineup composed only of one person. The suggestiveness of this identification procedure further supports disclosure of the additional photographs FACES generated and other information about the program's algorithm. *See, e.g.*, *Manson v. Brathwaite*, 432 U.S. 98, 116 (1977)

(due process requires suppression of evidence where the "indicators of [a witness's] ability to make an accurate identification" are outweighed by the corrupting effect of "the challenged identification itself.").[35]

Had the analyst shown the eyewitness a show-up of Mr. Lynch alone, it would have been "inherently suggestive," and would have required a trial court to conduct a full reliability analysis to determine whether the identification should be admitted as evidence. *Perez v. State*, 648 So.2d 715, 719 (Fla. 1995). "With good reason," including the danger that witnesses may "remember" the image in a photograph rather than the person they actually saw, the Supreme Court has "widely condemned[]" "such single-suspect procedures." *Manson*, 432 U.S. at 133 (citing *Stovall v. Denno*, 388 U.S. 293, 302 (1967); *Simmons v. United States*, 390 U.S. 377, 383–84 (1968)). Smaller lineups are more likely to be suggestive,[36] and commentators generally agree that they should contain at least six participants.[37]

---

[35] The typical remedy for an unduly suggestive identification is its suppression at trial. *Amici* contend that the likely suggestiveness of Mr. Lynch's identification lends further support for disclosure of information relevant to discerning whether the resulting identification should have been admitted at trial.

[36] *See, e.g., Ex parte Wimes*, 14 So.3d 131 (Ala. 2009) (where victim said he was attacked by two tall men, use of a 3-person lineup with only 2 tall men was "impermissibly suggestive"); *Commonwealth v. Wilson*, 301 A.2d 823 (Pa. 1973) (lineup of only the defendant and codefendant was impermissibly suggestive).

[37] *See* Nat'l Acad. of Sciences, *Identifying the Culprit: Assessing Eyewitness Identification*, 23, 28 (2011); U.S. Dep't of Justice, *Eyewitness Identification Procedures for Conducting Photo Arrays*, ¶ 3.1 (Jan. 6, 2017); Gary L. Wells, et

Numerous courts have excluded identifications based on less suggestive procedures than the one here—including when the defendant was the only person in a line-up who: was tall and wearing a leather coat;[38] had a particular accent;[39] had a certain type of facial hair;[40] wore a jail uniform;[41] or presented as a certain ethnicity with a specific build.[42] Here, Mr. Lynch was the *only* person whose likeness—along with his entire criminal history—was advanced for identification. In essence, the analyst showed a single photo to the witness while indicating that there was other evidence that the person pictured committed a crime—precisely the circumstances in which the Supreme Court has noted that the "danger of error is at its greatest." *Manson*, 432 U.S. at 133–34. Thus, the procedure by which Mr. Lynch's photo was identified was "unnecessarily suggestive," implicating broader due process concerns that Mr. Lynch should have been able to explore. *Fitzpatrick v. State*, 900 So.2d 495, 517 (Fla. 2005).

---

al., *Eyewitness Identification Procedures: Recommendations for Lineups and Photospreads*, 22 Law & Human Behav. 1, 7, 23–27 (1998); *State v. Lawson*, 352 Or. 724 (2012).

[38] *Foster v. California*, 394 U.S. 440, 443 (1969).

[39] *United States v. García-Álvarez*, 541 F.3d 8 (1st Cir. 2008).

[40] *United States v. Downs*, 230 F.3d 272 (7th Cir. 2000).

[41] *Moore v. State*, 900 P.2d 996 (Okla. 1995); *Jells v. Mitchell*, 538 F.3d 478 (6th Cir. 2008); *Haliym v. Mitchell*, 492 F.3d 680 (6th Cir. 2007).

[42] *Wurdemann v. State*, 390 P.3d 439 (Idaho 2017).

c. Officers' in-court identifications of Mr. Lynch do not cure the State's *Brady* violations.

United States Supreme Court precedent makes clear that the officers' in-court identifications of Mr. Lynch do not remedy the *Brady* violation. In *Kyles v. Whitley*, prosecutors withheld several pieces of *Brady* material, including inconsistent eyewitness identification statements and a computer print-out of license plate numbers from the crime scene that did not match the defendant's alleged plate. 514 U.S. at 429–30. Even though four witnesses each *twice* identified Kyles as the perpetrator in court, plus a blown-up picture of a car they argued belonged to Kyles, *id.* at 430–31, the Court held that the inconsistent eyewitness statements and computer printout, among other information, was *Brady* material and the prosecution's suppression of it merited reversal. *Id.* at 453–54.

The Court reasoned that the defense could have used that information to "attack[] the reliability of the investigation in failing even to consider [an alternate suspect's] possible guilt." *Id.* at 446. The Court recognized the importance of jurors' ability "to count the sloppiness of the investigation against the probative force of the State's evidence." *Id.* at 446 n.15. *See also Bowen v. Maynard*, 799 F.2d 593, 613 (10th Cir. 1986) ("A common trial tactic of defense lawyers is to discredit the caliber of the investigation or the decision to charge the defendant, and we may consider such use in assessing a possible *Brady* violation"); *Stano v. Dugger*, 901 F.2d 898, 903 (11th Cir. 1990) (citing *Bowen*); *Lindsey v. King*, 769

F.2d 1034, 1042 (5th Cir. 1985) (holding that withheld *Brady* evidence "carried within it the potential" for "discrediting" the police investigation).

Here, the analyst admitted she did not know vital details about the FACES program, including how it worked and the possible range—much less the certainty—of the star ratings, and testifying officers admitted to accepting the analyst's FACES-fueled recommendation without further investigation. (Sec Supp R I 21). Only after receiving that recommendation and Mr. Lynch's rap sheet did the officers identify the individual in the photo as Mr. Lynch. *Id.* This is far less investigation than took place in *Kyles*. Accordingly, the later in-court identifications of Mr. Lynch are not sufficient to outweigh the *Brady* violation.

The trial court erred in refusing to hold a hearing on the alleged *Brady* violation. *See Brown v. State*, 165 So.3d 726, 729 (Fla. 4th DCA 2015) (holding that a trial court has an affirmative obligation to hold a *Richardson* hearing upon learning of a possible discovery violation); *see also* Pet's Br. at 7–9. The trial court was put on notice of a possible discovery violation when Mr. Lynch sought the other potential matches generated by the algorithm, but failed to hold a hearing. Accordingly, this Court should exercise jurisdiction to resolve the conflict between the First District's holding here and *Brown* from the Fourth District.

CONCLUSION

For the foregoing reasons, this Court should accept jurisdiction of this case.

Respectfully submitted,

s/Benjamin James Stevenson
Benjamin James Stevenson
Fla. Bar. No. 598909
ACLU Found. of Fla.
3 W. Garden St., Suite 712
Pensacola, FL 32502-5636
T. 786.363.2738
bstevenson@aclufl.org

Counsel for Amici Curiae

Jennifer Lynch
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
T. 415.436.9333
jlynch@eff.org

Clare Garvie
Alvaro M. Bedoya
Center on Privacy & Technology
Georgetown University Law Center
600 New Jersey Ave NW
Washington, D.C. 20001
T. 202.661.6707
cag104@law.georgetown.edu

Alexis Agathocleous
Innocence Project, Inc.
40 Worth Street, Ste. 701
New York, New York 10013
T. 212.364.5968
agathocleous@innocenceproject.org

Vera Eidelman
Nate Wessler
Andrea Woods
Brandon Buskey
Brett Max Kaufman
Rachel Goodman
ACLU Foundation
125 Broad Street, 18th Fl.
New York, NY 10004
T. 212.549.2500
veidelman@aclu.org

Somil Trivedi
ACLU Foundation
915 15th Street, NW
Washington, DC 20005
T. 202.715.0802
strivedi@aclu.org

Of Counsel

CERTIFICATE OF SERVICE

I certify that the foregoing document has been furnished to the following persons on the E-filed date of this document by filing the document with service through the e-Service system (Fla.R.Jud.Admin. 2.516(b)(1)):

Trisha Meggs Pate (crimappdab@myfloridalegal.com), Counsel for the State

Victor Holder (victor.holder@flpd2.com, appeals_support@flpd2.com, appeals@flpd2.com), Counsel for Petitioner

s/Benjamin James Stevenson
Benjamin James Stevenson

CERTIFICATE OF COMPLIANCE

I certify that I used 14 point New Times Roman font in this brief; and therefore, it complies with the font requirements of Fla.R.App.P 9.210(a)(2).

/s/ Benjamin James Stevenson
Benjamin James Stevenson