Vanderbilt Journal of Entertainment & Technology Law

Volume 23 | Issue 4 Article 5

2021

Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom

Gabrielle M. Haddad

Recommended Citation

Gabrielle M. Haddad, Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom, 23 *Vanderbilt Journal of Entertainment and Technology Law* 891 (2021)

Available at: https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss4/5

Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom

ABSTRACT

From unlocking an iPhone to Facebook "tags," facial recognition technology has become increasingly commonplace in modern society. In the wake of the Black Lives Matter movement and call for police reform in the United States, it is important now more than ever to consider the implications of law enforcement's use of facial recognition technology. A study from the National Institute of Standards and Technology found that facial recognition algorithms generated higher rates of false positives for Black faces—sometimes up to one hundred times more false identifications—than white faces. Given the embedded bias of this technology and its increased prevalence, the lack of federal regulation of facial recognition technology and its uses by law enforcement are alarming. This Note explores issues that arise with law enforcement's use of facial recognition technology and how results from the technology should be treated in the criminal justice system.

This Note cautions against admitting results from facial recognition technology into evidence in criminal trials based on the current state of the industry and the technology. Further, if facial recognition evidence is admitted, this Note argues that defendants should have access to the software's source code to meaningfully challenge the evidence presented against them under the confrontation clause of the US Constitution. While this Note recognizes developers' interest in protecting trade secrets, it nevertheless recommends that judges balance these interests with those of defendants and make case-by-case decisions about how to protect developers' information without blocking defendants' access to the software.

TABLE OF CONTENTS

Robert Julian-Borchak Williams, a Black man from Michigan, was wrongfully arrested in January 2020 based on a flawed match from facial recognition technology.[1] Williams was minding his own business at work when he received a call from law enforcement asking him to come to the police station to be arrested. At first, he thought the call was a prank.[2] However, shortly after receiving this call, Williams was arrested on his lawn in front of his wife and two daughters.[3] The police would not explain why Williams was being arrested; they merely showed him a piece of paper reading "felony warrant" and "larceny" alongside his driver's license photo.[4] When his wife asked where he was being taken, an officer simply responded, "Google it."[5]

[1] Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/7GBH-ZH6Q] (last updated Aug. 3, 2020).

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

According to technology and legal experts, this may be the first known account of an American being wrongfully arrested based on a facial recognition algorithm.[6] Williams was arrested after a surveillance camera image of a man robbing a retail store was uploaded to a facial recognition system and generated multiple matches with Williams's driver's license photo among the results.[7] The results were shown to an eyewitness who had witnessed the crime five months prior and she selected Williams as the "correct" match.[8] Since Williams's arrest, US authorities have identified two other men wrongfully arrested based on facial recognition technology results; in each of these cases, the men mistakenly identified were Black.[9] These recent examples of police implementation of facial recognition technology raise questions about the technology's development and use.

The facial recognition technology that police departments employ to identify suspects predominantly originates from private companies. The National Institute of Standards and Technology (NIST) conducted a study in 2019 that evaluated 189 different algorithms from 99 developers, which represents the majority of the industry.[10] The study found that the algorithms generated higher rates of false positives for Black faces—sometimes up to one hundred times more false identifications—than white faces.[11] This study, and various others, reveal the widespread bias embedded in facial recognition technologies.[12]

In the context of the Black Lives Matter movement and call for police reform in the United States, it is important to consider the consequences of using biased facial recognition technology in law enforcement. The inaccuracy of facial recognition technology raises concerns about the potential disparate impact of this technology in law enforcement and the justice system. With the increasing use of this technology, it is likely that prosecutors will soon seek to introduce it

[6] *Id.*

[7] *Id.*

[8] *See id.*

[9] Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html [https://perma.cc/HHW3-XJTD] (last updated Jan. 6, 2021).

[10] *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, NAT'L INST. STANDARDS & TECH. [hereinafter *NIST Study*], https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software [https://perma.cc/A94Z-DGSY] (last updated May 18, 2020).

[11] Hill, *supra* note 1.

[12] *See id.*; *see also* Joy Buolamwini, Opinion, *When the Robot Doesn't See Dark Skin*, N.Y. TIMES (June 21, 2018), https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html [https://perma.cc/6NA2-2YQU].

into evidence at criminal trials to establish probable cause or as evidence of an identification.[13] Because this technology's embedded bias currently places minorities at a disadvantage in the criminal justice system, courts should carefully examine the state of the technology, its regulation, and consider what rights criminal defendants should have if condemning facial recognition technology evidence is introduced.

This Note addresses whether results from facial recognition technology should be admitted into evidence at trial and, if the results are admitted, what rights defendants should have to challenge this evidence. Part I gives background information on facial recognition technology, its use by law enforcement, and the lack of regulation. Part II examines whether results from facial recognition technology are admissible as reliable scientific evidence under the *Daubert* factors and analyzes the scope of defendants' right to challenge the evidence if admitted. Part III suggests that results from facial recognition technology should not be admitted into evidence at trial based on the *Daubert* factors and further recommends legislation that would grant defendants access to the software used in their trials, with possible protections for the software developer's trade secrets.

I. BACKGROUND

A. The Black Lives Matter Movement

The Black Lives Matter movement gained substantial traction in the United States on May 25, 2020, when George Floyd, a 46-year-old Black man from Minneapolis, was killed by a Minneapolis police officer.[14] Police officers responded to a call that claimed Floyd paid for a pack of cigarettes with a counterfeit $20 bill.[15] Floyd allegedly resisted the officers when they handcuffed him, resulting in a white police officer pinning Floyd to the ground with his knee on Floyd's neck.[16] Despite Floyd's repeated cries, "I can't breathe," the officer did not release his knee from Floyd's neck for eight minutes and forty-six seconds, resulting in Floyd's death. Bystanders captured this encounter on camera. Shortly after Floyd's death, videos of the officer's knee on

[13] Kristine Hamann & Rachel Smith, *Facial Recognition Technology: Where Will It Take Us?*, 34 AM. BAR ASS'N CRIM. JUST. MAG. (Apr. 15, 2019), https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/ [https://perma.cc/7K9B-JQGA].

[14] *See What to Know About the Death of George Floyd in Minneapolis*, N.Y. TIMES (Mar. 2, 2021), https://www.nytimes.com/article/george-floyd.html [https://perma.cc/YS6E-4HRJ].

[15] *Id.*

[16] *Id.*

Floyd's neck sparked outrage across the United States; citizens across the country took to the streets to protest police brutality and systemic racism in the weeks and months that followed.[17]

However, Floyd's death is not an isolated incident. Many in the Black Lives Matter movement drew comparisons to the death of Eric Garner. Garner was a Black man who died in police custody in New York City in 2014 after an officer held him in a chokehold.[18] Garner repeatedly pleaded, "I can't breathe." Like Floyd, Garner's death was also video recorded by a bystander. This plea, "I can't breathe," has become a rallying cry for the Black Lives Matter movement.[19] Floyd and Garner are only two of the large number of Black victims of police brutality that have become the faces of the Black Lives Matter movement.

The killings of George Floyd and Eric Garner demonstrate the dangerous correlation between systemic racism and police brutality. As the Black Lives Matter movement continues to publicly confront this correlation, it is imperative to also confront the disparate impact of the use of facial recognition technology in policing. As this technology pervades our society, its embedded bias[20] is problematic for minorities who have historically been disproportionately targeted by law enforcement.[21] The potential for facial recognition technology to further disadvantage minorities in the criminal justice system warrants a deeper examination of police methodology for using the technology and increased judicial scrutiny of its use as evidence in a criminal proceeding.

B. Facial Recognition Technology Generally

The use of facial recognition technology is increasingly common in modern society. Facial recognition is the process of comparing two

[17] *Id.*

[18] *See* Deborah Bloom & Jareen Imam, *New York Man Dies After Chokehold by Police*, CNN, https://www.cnn.com/2014/07/20/justice/ny-chokehold-death/index.html [https://perma.cc/KAD7-TGP7] (last updated Dec. 8, 2014, 5:31 PM).

[19] *See id.*; Benazir Wehelie & Amy Woodyatt, *'I Can't Breathe': Hundreds Lie Down in Protest*, CNN, https://www.cnn.com/2020/06/03/world/gallery/george-floyd-lie-down-intl-scli/index.html [https://perma.cc/R4VJ-47AR] (last updated June 4, 2020, 7:19 AM).

[20] *See* Hill, *supra* note 1 (describing a study that found that the algorithms generated higher rates of false positives for Black faces—sometimes up to one hundred times more false identifications—than Caucasian faces).

[21] *See* Drew Desilver, Michael Lipka & Dalia Fahmy, *10 Things We Know About Race and Policing in the U.S.*, PEW RSCH. CTR.: FACT TANK (June 3, 2020), https://www.pewresearch.org/fact-tank/2020/06/03/10-things-we-know-about-race-and-policing-in-the-u-s/ [https://perma.cc/YK2Q-7NRM].

images of faces to determine whether they represent the same person.[22] Facial recognition technology operates by first recognizing a face and then measuring its features.[23] The algorithm identifies different landmarks on a person's face that can be quantified, such as distance between the eyes, width of the nose, and depth of the eye sockets.[24] After taking these measurements, the software uses these landmarks to create a template to compare to preexisting images of known faces.[25] The algorithm analyzes pairs of faces and generates a score reflecting the similarity of the faces' features.[26] Facial recognition is probabilistic; the technology produces more or less likely matches, not definitive matches.[27] These technologies "learn" over time as they are trained through exposure to large amounts of data and begin to infer rules from the patterns that emerge.[28]

C. Law Enforcement Use of Facial Recognition Technology

Facial recognition technology has proliferated many industries, and law enforcement is no exception. Law enforcement facial recognition networks include over 117 million American adults.[29] Because facial recognition databases include so many Americans, it is alarming that the use of this technology is essentially unregulated. There are currently no federal statutes that govern the use of facial recognition technology.[30] Some state and local governments have stepped in to regulate where Congress has not, but most of their regulations have addressed general biometric information without specifics on facial recognition technology.[31]

The Georgetown Law Center on Privacy and Technology conducted a year-long investigation of police departments across the

[22] *See* Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIV. & TECH. (Oct. 18, 2016), https://www.perpetuallineup.org/ [https://perma.cc/66QN-LUJ4].

[23] *See* Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work*, HOW STUFF WORKS, https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm [https://perma.cc/8EQL-U4G8] (last visited Feb. 22, 2021).

[24] *See id.*

[25] *See* Hamann & Smith, *supra* note 13.

[26] *See id.*

[27] *See* Garvie et al., *supra* note 22.

[28] *See* Patrick W. Nutter, Comment, *Machine Learning Evidence: Admissibility and Weight*, 21 U. PA. J. CONST. L. 919, 927–28 (2019).

[29] Garvie et al., *supra* note 22.

[30] Elizabeth McClellan, *Facial Recognition Technology: Balancing the Benefits and Concerns*, 15 J. BUS. & TECH. L. 363, 365 (2020).

[31] *Id.*

country and published a report with the following striking statistics on the departments' use of facial recognition technology:

- At least one of four state or local police departments has the option to run facial recognition searches through their system or another agency's system.[32]
- At least twenty-six states allow law enforcement to run or request searches on their databases of driver's license and identification photos, and these databases primarily contain information about law-abiding Americans.[33]

States allow police departments to search databases that contain information about law-abiding Americans, exposing a significant transition in law enforcement investigations.[34] Police have traditionally used fingerprint and DNA databases that are composed of information from criminal arrests and investigations.[35] Now they are using driver's license databases, tapping into a resource with information primarily from law-abiding Americans.[36] Facial recognition searches have become routine at the federal and state level.[37] The Georgetown report offers numbers on a few particular facial recognition systems: Ohio's system was used 6,618 times by 504 agencies in its first eight months of operation while the San Diego Association of Government's system is used by San Diego agencies for an average of about 560 searches each month. Pinellas County's system in Florida is used to conduct around 8,000 searches per month.[38] Further, the Georgetown report outlines four common ways that police use facial recognition technology: (1) stop and identify, (2) arrest and identify, (3) investigate and identify, and (4) real-time video surveillance.[39]

Despite serious concerns, facial recognition technology has been useful for law enforcement in criminal case investigations.[40] Police have used facial recognition evidence, along with other evidence, to establish probable cause for arrest for passport fraud and in identity theft cases.[41] The New York Police Department used facial recognition software on a surveillance image of a shooter in a nightclub to arrest him in 2017.[42]

[32] Garvie et al., *supra* note 22.

[33] *Id.*

[34] *See id.*

[35] *Id.*

[36] *See id.*

[37] *See id.*

[38] *Id.*

[39] *Id.*

[40] *See* Hamann & Smith, *supra* note 13.

[41] *Id.*

[42] *Id.*

Police were able to narrow down the two hundred likely matches that the software generated by comparing the images and looking for similar physical characteristics between them; the department then presented a photo array to witnesses to identify the shooter.[43]

While law enforcement agencies are increasingly integrating facial recognition technology into their daily operations, they are not implementing sufficient safeguards to ensure the accuracy of their systems.[44] Most law enforcement agencies contract with private companies that provide facial recognition software. One major facial recognition company, FaceFirst, publicly advertised a 95 percent accuracy rate for its facial recognition technology but then expressly disclaimed liability for failing to meet that threshold in contracts with the San Diego Association of Governments.[45] This raises questions about the accuracy of the technologies created by these private companies. Most police departments rely on their officers to verify that the technology has made an accurate match between the image submitted to the technology and the image from its database.[46] However, a recent study has shown that users make the wrong decision about a match about half of the time if they have not had specialized training in facial identification.[47]

D. Private Facial Recognition Companies

Private companies generally provide law enforcement agencies with their facial recognition technology. The only public benchmark to assess the accuracy of facial recognition algorithms is a completely voluntary competition that the NIST offers every three to four years.[48] Private companies are not required to participate in this competition at all, even if they are selling their facial recognition technology to law enforcement.[49] This evidences a gaping hole in the regulation of private facial recognition technologies—there are no current standards that ensure their algorithms are accurate. This is especially concerning given the bias embedded in facial recognition technology, resulting in its increased inaccuracy when identifying minority faces.[50]

[43] *Id.*

[44] *See* Garvie et al., *supra* note 22.

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] *See id.*

[49] *See id.*

[50] *See* Buolamwini, *supra* note 12.

Further, the government does not directly regulate private facial recognition companies' data collection that is used to create and train their algorithms. There are some state laws that indirectly regulate facial recognition technology, like the Illinois Biometric Information Privacy Act (BIPA). BIPA implicates facial recognition data in its aim to protect biometric information in general. However, BIPA does not specifically address facial recognition technology. BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade or otherwise obtain" someone's biometric identifiers unless that person is informed.[51] BIPA defines "biometric identifier" as an eye scan, fingerprint, voiceprint, hand scan, or face geometry.[52]

Clearview AI is a facial recognition company that has contracts with more than six hundred law enforcement agencies across the country.[53] Clearview has collected data from Facebook, Venmo, YouTube, and Twitter and amassed three billion images for its facial recognition technology.[54] The invasive nature of this data scraping is alarming and has led to a number of lawsuits claiming that companies collecting personal data like this have violated BIPA.[55] Specifically, the American Civil Liberties Union (ACLU) filed a suit against Clearview because of the company's alleged illegal collection and storage of Illinois citizens' faceprints without their knowledge or consent. Further, the ACLU alleged that Clearview sold the data to private companies and law enforcement, which enables law enforcement to use this data for facial recognition purposes.[56] Because law enforcement's use of facial recognition technology is vastly unregulated, the access that law enforcement has to large amounts of private data is disturbing.

Other states, such as Texas and Washington, have also enacted laws to protect biometric information where the federal government has

[51] 740 ILL. COMP. STAT. ANN. 14/15(b) (West 2020).

[52] *Id.* 14/10.

[53] *CEO of AI Startup Dismisses Critics*, CBS THIS MORNING (Feb. 5, 2020), https://www.cbs.com/shows/cbs_this_morning/video/5EMDCMqNXNddglebBhlvpHYrJUk1lOaw/ceo-of-controversial-ai-startup-dismisses-critics/ [https://perma.cc/KZ5R-353Z].

[54] *Id.*

[55] *See* Nick Statt, *ACLU Sues Facial Recognition Firm Clearview AI, Calling It a 'Nightmare Scenario' for Privacy*, VERGE (May 28, 2020, 1:13 PM), https://www.theverge.com/2020/5/28/21273388/aclu-clearview-ai-lawsuit-facial-recognition-database-illinois-biometric-laws [https://perma.cc/634X-D9QB]; Taylor Hatmaker, *Lawsuits Allege Microsoft, Amazon and Google Violated Illinois Facial Recognition Privacy Law*, TECHCRUNCH (July 15, 2020, 4:59 PM), https://techcrunch.com/2020/07/15/facial-recognition-lawsuit-vance-janecyk-bipa/ [https://perma.cc/7H77-UN7C].

[56] Complaint at 3–4, Am. C.L. Union v. Clearview AI, Inc., No. 2020-CH-04353 (Ill. Cir. Ct. May 28, 2020); *see* Statt, *supra* note 55.

not.[57] These state laws do not regulate facial recognition technology and its uses, but rather the data itself. Recently, San Francisco became the first city to ban facial recognition technology use by its state agencies in May 2019.[58] In the findings section of the ordinance, the city expressed concern that facial recognition technology has the ability to endanger civil rights in a way that outweighs the benefits of the technology. According to the ordinance, citizens should have the ability to live free of continuous government monitoring.[59] Further, the ordinance points out that this technology exacerbates racial injustice because of the disproportionate accuracy rates for different demographics.[60]

E. Congressional Action

Local and state governments are beginning to step in to regulate where Congress has not. Even though there is a lack of federal legislation to regulate facial recognition technology, Congress has held hearings and proposed bills on the subject.[61] To date, Congress has not passed any legislation to regulate facial recognition technology; yet the amount of legislation congressional members have proposed over recent years signifies an appetite in the legislature to regulate the problematic side effects of this technology.

In 2019, the 116th Congress held two hearings on facial recognition technology.[62] As a result, two federal bills were proposed: the Commercial Facial Recognition Privacy Act of 2019 and the Facial Recognition Technology Warrant Act.[63] The Commercial Facial Recognition Privacy Act would require businesses to obtain consent from consumers before employing facial recognition technology.[64] This Act did not specifically address law enforcement. The Facial Recognition Technology Warrant Act, on the other hand, would have required law enforcement to obtain a warrant based on probable cause before using facial recognition technology for ongoing

[57] S. REPUBLICAN POL'Y COMM., 116TH CONG., FACIAL RECOGNITION: POTENTIAL AND RISK (Nov. 20, 2019), https://www.rpc.senate.gov/policy-papers/facial-recognition-potential-and-risk [https://perma.cc/LGL2-7TR7].

[58] S.F., CAL., ADMIN. CODE ch. 19B, § 19B.1, ch. 21, § 21.07 (2020).

[59] S.F., Cal., Ordinance 107-19 § 1(d) (May 21, 2019).

[60] *Id.* § 1(c); *see* Hill, *supra* note 1.

[61] S. REPUBLICAN POL'Y COMM., *supra* note 57.

[62] *Id.*

[63] *Id.*

[64] *Id.*

surveillance.[65] Moreover, this Act would have limited surveillance to thirty days and set additional rules to minimize the data collected on people outside a warrant.[66]

In particular, a bill introduced in 2019 called the Justice in Forensic Algorithms Act targeted issues associated with law enforcement using forensic algorithms and introducing these algorithms at trial to condemn a defendant. The bill established standards and testing requirements for general use of forensic algorithms and addressed forensic evidence at trial.[67] The bill charged the NIST to establish Computation Forensic Algorithms Standards and a Computational Forensic Algorithms Testing Program that federal law enforcement must comply with when using forensic algorithms.[68] The bill outlined the NIST standards to include an assessment for potential disparate impact on different demographics, requirements for software testing, requirements for developers' public disclosure of documentation about the software (including information about the development process and its training data), and requirements to provide defendants with reports that document the use and results of the forensic software program in their trials.[69] NIST's Testing Program required testing in accordance with the NIST standards, that testing use realistic data sets that represent diverse racial and ethnic groups, and that the test results were published online with specifics about the software's performance on diverse populations.[70] The bill provided that evidence from forensic software would only be admissible in a criminal case if the software were to be submitted to the NIST testing program.[71]

Further, by proposing that developers cannot assert a trade secret privilege to block defendants, this bill protected defendants' access to algorithms' source codes where the algorithms are used in a criminal trial.[72] The bill created a blanket rule that trade secret protections do not apply in criminal trials "when defendants would otherwise be entitled to obtain evidence" by amending the Federal

[65] *Id.*

[66] Dennis Romboy, *Sen. Mike Lee to Police Doing Facial Recognition Surveillance: Get a Warrant*, DESERET NEWS (Nov. 14, 2019, 7:36 PM), https://www.deseret.com/utah/2019/11/14/20965330/sen-mike-lee-to-police-doing-facial-recognition-surveillance-get-a-warrant [https://perma.cc/GQT5-UKUV].

[67] *See* H.R. 4368, 116th Cong. (2019).

[68] *See id.* § 2.

[69] *See id.* § 2(a).

[70] *See id.* § 2(d).

[71] *See id.* § 2(g).

[72] *See id.* § 2(a).

Rules of Evidence.[73] Moreover, defendants would receive a report on the software used in their cases and would be given access to the software so they can test it.[74] Because of the extreme nature of this blanket rule on trade secret protections, the bill did not gain traction to pass.[75]

A final piece of federal legislation—the George Floyd Justice in Policing Act—was proposed on the House Floor in June 2020 to regulate police departments.[76] The bill passed in the House, but did not pass in the Senate.[77] A notable part of this legislation that specifically applied to facial recognition technology—the Federal Police Camera and Accountability Act—required police officers to wear body cameras to conduct their searches and make their arrests but prohibited officers from equipping or employing facial recognition technology on their body cameras.[78] Further, any footage from their body cameras was not to be subject to facial recognition technology.[79] The proposed bill imposed broad regulations on police departments to increase transparency and accountability, with the goal of reducing discriminatory practices.[80] The bill, however, did not pass through the Senate because of partisan disagreements.[81]

F. Facial Recognition Evidence at Trial

Facial recognition evidence has not yet been introduced at trial.[82] However, with increasing use of the technology, it is likely that prosecutors will begin to introduce this technology as evidence to establish probable cause or as evidence of an individual's identification.[83] In this context, evidentiary questions will likely emerge about the scientific reliability of facial recognition technology, which

[73] *Id.* § 2(b).

[74] Press Release, Mark Takano, House of Representatives, Rep. Takano Introduces the Justice in Forensic Algorithms Act to Protect Defendants' Due Process Rights in the Criminal Justice System (Sept. 17, 2019), https://takano.house.gov/newsroom/press-releases/rep-takano-introduces-the-justice-in-forensic-algorithms-act-to-protect-defendants-due-process-rights-in-the-criminal-justice-system [https://perma.cc/7QY7-M7AH].

[75] *See* H.R. 4368, 116th Cong. (2019).

[76] *See* George Floyd Justice in Policing Act of 2020, H.R. 7120, 116th Cong. (2020).

[77] *See id.*

[78] *Id.* §§ 372, 374.

[79] *Id.* § 374.

[80] *See* H.R. REP. NO. 116-434, at 37–38 (2020).

[81] *See* Li Zhou & Ella Nilsen, *The House Just Passed a Sweeping Police Reform Bill*, VOX (June 25, 2020, 8:50 PM), https://www.vox.com/2020/6/25/21303005/police-reform-bill-house-democrats-senate-republicans [https://perma.cc/42CS-VSVM].

[82] *See* Hamann & Smith, *supra* note 13.

[83] *Id.*

must be established under the *Frye* or *Daubert* standard before the evidence is admitted.[84]

There is an array of issues that arises regarding the reliability of facial recognition technology evidence. For instance, the technology has limitations on its accuracy given the conditions of the photos being analyzed.[85] The technology works best when photos are taken head-on with good lighting and no movement.[86] Consequently, the accuracy of the technology decreases when there is no standardized photo for comparison or when a photo was taken in an uncontrolled environment, perhaps from a different angle with low-quality lighting.[87] Further, the evolving nature of faces and appearances affects the accuracy of the technology because of changes like a new hairstyle, facial hair growth, weight gain or loss, and aging.[88] Many facial recognition systems are also less accurate when reading faces of certain demographics, specifically Black people.[89]

Moreover, the proprietary nature of this technology is problematic when analyzing whether a facial recognition technology has been reviewed by other experts in the field.[90] Many police departments contract with private companies that are not willing to disclose their trade secrets.[91] To address these concerns, this Note conducts an analysis of the reliability of evidence from facial recognition technology under the *Daubert* factors.[92]

II. ANALYSIS

A. Facial Recognition Technology Admissibility as Evidence

Federal Rule of Evidence 702 governs whether an expert witness's testimony is admitted into evidence, and was effectively created, in part, by the Court's decision in *Daubert v. Merrell Dow*

[84] *Id.*

[85] *See id.*

[86] *Id.*

[87] *Id.*

[88] *Id.*

[89] *Id.*; Buolamwini, *supra* note 12; *NIST Study*, *supra* note 10.

[90] *See* John Nawara, *Machine Learning: Face Recognition Technology Evidence in Criminal Trials*, 49 U. LOUISVILLE L. REV. 601, 614 (2011).

[91] *Id.*

[92] This Note uses the *Daubert* standard because it is used more frequently than the *Frye* standard in many state and federal courts. *See Frye Standard*, CORNELL L. SCH. LEGAL INFO. INST, https://www.law.cornell.edu/wex/frye_standard [https://perma.cc/4CXD-8R6E] (last visited Feb. 23, 2021).

Pharmaceutical, Inc.[93] Because federal courts adhere to *Daubert* to assess the reliability of expert evidence, this Note uses the *Daubert* factors to analyze the admissibility of results from facial recognition technology. In *Daubert*, the Supreme Court established a set of factors to assess the reliability of scientific expert testimony.[94] This new test was meant to establish a "gatekeeping" role for federal courts in determining what evidence should be admitted.[95] The non-exhaustive list of factors that the *Daubert* Court provided are (1) whether the technique can be or has been tested; (2) whether the technique has been subjected to peer review and publication; (3) the technique's known or ascertainable rate of error; (4) whether there are recognized standards for using the technique; and (5) whether the technique has been generally accepted in the relevant specialty scientific fields.[96]

In subsequent decisions, the Court has clarified that the inquiry is not about the general validity of the expert's discipline.[97] Rather, the inquiry is specifically about the reliability of the particular technique that the expert relies on in his testimony.[98] This Note applies this list of *Daubert* factors to facial recognition technology to consider whether this type of evidence should be admitted in trial. Ultimately, this Note concludes that it should not be admitted into trial as evidence based on the current state of the technology and the lack of regulation.

1. Factor One: Testability

Facial recognition technology is easily testable.[99] In general, it is much easier to test a mathematical system that takes measurements and produces results rather than, for example, a sociological theory.[100] Facial recognition technology produces results that can easily be shown to be false. It is possible to create experiments that estimate how likely a system is to result in false positive or false negative results.[101] One disturbing example of the testability of facial recognition technology is Google's recognition system that falsely identified two Black

[93] FED. R. EVID. 702 advisory committee's note to 2000 amendment; Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579 (1993).

[94] *Daubert*, 509 U.S. at 592–94.

[95] Mohammed Osman & Edward Imwinkelried, *Facial Recognition Systems*, 50 CRIM. L. BULL., no. 3, 2014, at 695.

[96] *Daubert*, 509 U.S. at 593–94.

[97] Osman & Imwinkelried, *supra* note 95; *see* Gen. Elec. Co. v. Joiner, 522 U.S. 136 (1997); Kumho Tire Co. v. Carmichael, 526 U.S. 137 (1999).

[98] Osman & Imwinkelried, *supra* note 95.

[99] *Id.*

[100] *See* Nawara, *supra* note 90, at 612.

[101] Osman & Imwinkelried, *supra* note 95.

individuals as gorillas in 2015, resulting in public criticism and outcry to improve the system.[102]

Even though facial recognition technology *can be* easily tested, there is another aspect of this factor: whether the technology actually *has been* tested and what the results were.[103] As explored above, there is no mandatory testing of facial recognition technology.[104] The NIST offers a voluntary facial recognition technology competition, but facial recognition technology companies are not required by any governing body to test their technology.[105] It is reasonable to think that companies will proactively test their technology to refine their products, but these internal test results are not publicly available. It is evident that facial recognition technology has been tested because of the variety of studies that have evaluated its accuracy, but this sporadic testing is not adequate.[106]

The NIST has published the most comprehensive reports on tests and evaluations of facial recognition technology. NIST's Face Recognition Vendor Test (FRVT) Program produces studies and reports on different aspects of the technology.[107] Importantly, NIST's FRVT program evaluates algorithms that are submitted by research and development laboratories.[108] These algorithms are not necessarily available as products, but rather are prototypes.[109] Therefore, this testing can only speak to the reliability of facial recognition prototypes, not the actual technology that is used and implemented.[110] This weakens the claim that facial recognition technology should be admitted into trial as evidence because the most comprehensive reports on facial recognition technology and its accuracy test prototypes, not final products.

Facial recognition technology's embedded bias is one particular concern that has arisen as a result of testing the technology.[111] Part 3 of the NIST FRVT program evaluated the accuracy of facial recognition

[102] Nutter, *supra* note 28, at 933.

[103] Osman & Imwinkelried, *supra* note 95.

[104] *See* discussion *supra* Section I.D.

[105] *See* Garvie et al., *supra* note 22.

[106] *See NIST Study*, *supra* note 10; Buolamwini, *supra* note 12.

[107] *See Face Recognition Vender Test (FRVT)*, NAT'L INST. STANDARDS & TECH., https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt [https://perma.cc/8U8V-EXE2] (last visited Feb. 23, 2021).

[108] PATRICK GROTHER, MEI NGAN & KAYEE HANAOKA, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., FACE RECOGNITION VENDOR TEST (FRVT) PART 3: DEMOGRAPHIC EFFECTS 1 (2019), https://doi.org/10.6028/NIST.IR.8280 [https://perma.cc/8VSA-4WRW].

[109] *Id.*

[110] *See id.*

[111] *See id.* at 4, 14–15; Buolamwini, *supra* note 12.

algorithms with different demographic groups.[112] The study tested algorithms from the majority of the industry and found that algorithms generated higher rates of false positives for Black faces—sometimes up to one hundred times more false identifications—than white faces.[113] Even though the accuracy of facial recognition technology will improve over time, the current bias in these systems is concerning and weakens the claim that it should be allowed into trial as evidence.

2. Factor Two: Peer Review and Publication

There is no question that there is an abundance of literature on facial recognition technology. The scientific community has written about this technology and explored its uses and applications. However, the proprietary nature of facial recognition technology raises questions about the level of scrutiny applied to it.[114] Because police departments contract with private companies for facial recognition technology, there are concerns about how meaningfully the academic community can feasibly analyze these companies' technologies without access to the inner workings of the software.[115] This concern cuts against admitting facial recognition technology as evidence because disclosure of the technology's source code is necessary to evaluate the reliability of the technology.[116]

3. Factor Three: Rate of Error

There are two different error rates to consider with facial recognition technology.[117] The first error rate is described with the embedded bias of the technology: the error rate with respect to training data.[118] This error rate leads to increased performance over time by using machine learning and better data to train the algorithm.[119] The second error rate is the inaccuracy that ensues when an algorithm is unleashed in the real world with unknown conditions where photos may not be taken in the standard way that the algorithm has been trained.[120] There may be poor lighting, or the photo may be taken from an angle

[112] GROTHER ET AL., *supra* note 108, at 30–33.

[113] *NIST Study*, *supra* note 10.

[114] *See* Nawara, *supra* note 90.

[115] *Id.*

[116] *See* Christian Chessman, Note, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CALIF. L. REV. 179, 215–19 (2017).

[117] Nutter, *supra* note 28, at 933.

[118] *Id.*

[119] *Id.*

[120] *Id.*

without a full view of the subject's face.[121] Further, a particular error rate may not speak to the technology's accuracy when it is applied to a person who does not share characteristics with the initial training data.[122] As mentioned above, facial recognition technology is frequently trained on data sets that are not diverse.[123] Therefore, the technology's error rate may be much higher when applied to an individual of color.[124]

It is difficult to judge the most accurate error rate because of the different possible error rates that may be reported and the variability of error rates when applied to subjects with different appearances.[125] A technology with a nondiverse data set may be fairly accurate when applied to a white individual. However, when it is applied to a Black individual, it is doubtful that the expert has complied with FRE 702(d) and "reliably applied the principles and methods to the facts of the case."[126]

4. Factor Four: Standards

There are no standards set out to control the development and operation of facial recognition technology.[127] Companies develop their own facial recognition technology and keep their information to themselves.[128] Therefore, standards have not developed in this industry and this is problematic for facial recognition systems.[129] This factor is straightforward because there are no published standards for facial recognition technology, and this factor weakens the argument that facial recognition technology evidence should be admitted into trial as evidence.[130]

5. Factor Five: General Acceptance

Machine learning is generally accepted,[131] and there is an array of facial recognition protocols and tests that has also been generally accepted in the scientific community.[132] However, the proprietary

[121] *See id.* at 931–34.

[122] *Id.* at 934.

[123] *Id.*

[124] *Id.*

[125] *Id.* at 934–35.

[126] *Id.* at 935.

[127] *See* Osman & Imwinkelried, *supra* note 95.

[128] *See id.*

[129] *See id.*

[130] *See id.*

[131] *See* Nutter, *supra* note 28, at 933.

[132] *See* Nawara, *supra* note 90, at 615–16.

nature of this technology is, again, concerning; the particular methods for the evidence introduced are not disclosed by the private companies who own this technology.[133]

Under the five *Daubert* factors alone, it is unlikely that results from facial recognition technology will be allowed into evidence at trial.[134] These five factors, however, do not constitute an exhaustive list; courts may consider other factors when evaluating the admissibility of expert witness testimony. Therefore, even if the results from facial recognition technology would not be admissible under the five factors listed in *Daubert*, courts may nonetheless admit these results into evidence.[135] If results from facial recognition technology are admitted into evidence, the defendant has the right to challenge and cross-examine.[136]

B. Contestability of Facial Recognition Technology Evidence

Just because evidence has been deemed "reliable" under the *Daubert* inquiry does not mean that the evidence is correct.[137] The *Daubert* factors ask about the reliability of the scientific expert's methodology in reaching a conclusion, but the correctness of the conclusion itself must be evaluated in the adversarial process.[138] Legal scholars refer to cross-examination as the "greatest legal engine ever invented for the discovery of truth."[139] Thus, defendants have a significant interest in contesting evidence from a facial recognition technology system that could be inaccurate.[140]

[133] *Id.* at 614.

[134] *See* discussion *supra* Section II.A.

[135] *See* Osman & Imwinkelried, *supra* note 95.

[136] Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1375 & n.166 (2018) (stating that the FED. R. EVID. 702 advisory committee's note to the 2000 amendment observes "that 'rejection of expert testimony is the exception rather than the rule' and that the court's gatekeeper function should not substitute for the role of the adversary system").

[137] Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 596 (1993) ("Vigorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence.").

[138] *Cf.* Edward J. Imwinkelried, *Computer Source Code: A Source of the Growing Controversy over the Reliability of Automated Forensic Techniques*, 66 DEPAUL L. REV. 97, 119 (2017).

[139] JOHN HENRY WIGMORE, 5 EVIDENCE IN TRIALS AT COMMON LAW § 1367 (James H. Chabourn ed., Little, Brown & Co. 1974).

[140] *See* Rebecca Wexler, *Convicted by Code*, SLATE (Oct. 6, 2015, 12:28 PM), https://slate.com/technology/2015/10/defendants-should-be-able-to-inspect-software-code-used-in-forensics.html [https://perma.cc/BVF3-NDPK].

The Sixth Amendment's confrontation clause states that "[i]n all criminal prosecutions, the accused shall have the right . . . to be confronted with the witnesses against him."[141] In practice, this clause requires witnesses to be present at trial to be cross-examined so that the defendant may confront his accuser.[142] Given a defendant's right to confront his accuser, this policy favors giving defendants the right to challenge the source code of the facial recognition technology because it is the processes of the technology that generate the condemning result.

1. Defendant's Right to Cross-Examine Facial Recognition Source Code

The foundation of our adversarial system relies on cross-examining human witnesses; this traditional system of confrontation has not, to date, caught up with the standardization of technology in our society.[143] New technologies present "process-based" evidence which is dependent on a machine using its standardized processes.[144] Rather than confronting lay and expert witnesses, defendants are often challenged with confronting machine witnesses. This is starkly different from the typical eyewitness testimony for which the confrontation clause was designed. Therefore, the reliability of machine witnesses demands a different type of analysis.[145]

The Supreme Court held in *Melendez-Diaz v. Massachusetts* that certified forensic lab reports are testimonial evidence and are inadmissible unless accompanied by a lab technician who can certify and attest to the validity of the report.[146] As a result of this holding, a forensic technician must testify in court and be subject to cross-examination.[147] However, the confrontation clause may not be satisfied by a lab technician testifying on behalf of a process-based technology.[148] The appropriate target of cross-examination is the standardized process, not the lab technician.[149] The process itself, not the technician's observations or negligible involvement, accuses the defendant.[150]

[141] U.S. CONST. amend. VI.

[142] Edward K. Cheng & G. Alexander Nunn, *Beyond the Witness: Bringing a Process Perspective to Modern Evidence Law*, 97 TEX. L. REV. 1077, 1093 (2019).

[143] *See id.* at 1092–93.

[144] *Id.* at 1088–89.

[145] *Cf. id.*

[146] *Id.* at 1094; Melendez-Diaz v. Massachusetts, 557 U.S. 305, 308, 311, 329 (2009).

[147] Cheng & Nunn, *supra* note 142, at 1094–95.

[148] *See id.* at 1095.

[149] *Id.*

[150] *Id.*

Defendants have a right to challenge the evidence presented against them in a meaningful way. Thus, it is important to think about the specifics of challenging facial recognition technology evidence. Source code is the "heart" of a computer program.[151] This code contains all the instructions for the technology to operate, dictates which tasks it will perform, and determines how it will perform them.[152] Gaining access to the technology's source code would be the most meaningful way for the defendant to challenge facial recognition technology because it would reveal information about the algorithm's inner workings that private companies keep to themselves.[153]

Having access to the source code of a program is comparable to "looking under the hood" of a car, which is distinct from watching a car drive.[154] While someone can learn limited details from observing a moving vehicle, the observer cannot understand the true inner workings of a car without looking under the hood.[155] The Volkswagen cheating scandal is particularly illustrative. In 2015, Volkswagen admitted that it had rigged its software—its secret code—so that its diesel cars would pass emissions tests when they actually did not meet the EPA's requirements.[156] The people who inspected Volkswagen's cars had no idea that the software's pollution-control equipment kicked in only during inspections.[157] The software took cues from the position of the steering wheel, the speed of the vehicle, and how long the engine was running to detect an ongoing inspection and then turned on the pollution-control mechanism.[158] The inspectors were able to watch the car drive, but they were oblivious to the deceitful inner workings of the proprietary software.[159] It is the same for computer programs and technologies; an observer learns limited information from watching the program in action.[160] The source code is necessary to know about the technology's processes.[161]

A secret algorithm that offers a condemning result is like evidence offered by an anonymous expert, whom a defendant cannot

[151] Imwinkelried, *supra* note 138, at 98.

[152] *Id.* at 98–99.

[153] Chessman, *supra* note 116, at 182–83.

[154] *Id.*

[155] *Id.*

[156] Jim Dwyer, *Volkswagen's Diesel Fraud Makes Critic of Secret Code a Prophet*, N.Y. TIMES (Sept. 22, 2015), https://www.nytimes.com/2015/09/23/nyregion/volkswagens-diesel-fraud-makes-critic-of-secret-code-a-prophet.html [https://perma.cc/6Q2A-3Y5L].

[157] *Id.*

[158] *Id.*

[159] *See id.*

[160] Chessman, *supra* note 116, at 182–83.

[161] *See id.*

cross-examine.[162] The confrontation clause clearly provides defendants the right to cross-examine their accusers; accordingly, defendants should have access to the source code of the technologies that accuse them.[163]

However, facial recognition technology and its processes are proprietary in nature. Private companies do not disclose the processes and intricacies of their technology because they are competing in a marketplace with other companies. Therefore, a facial recognition company claiming its source code to be a trade secret to avoid disclosing it to the court is a foreseeable obstacle for defendants who may want to challenge results from facial recognition technology.

2. Developers' Trade Secret Privilege

The rationale behind allowing companies to invoke a trade secret privilege is to encourage innovation and to discourage unfair business practices.[164] For a company, the first step in successfully invoking the trade secret privilege is to show that one has a valid trade secret under the jurisdictional requirements.[165] In the context of criminal cases, there is a lower likelihood that criminal defendants will have the resources to challenge a claimant's asserted privilege.[166] Therefore, it is safer for companies to assert the privilege in the criminal context, and companies are more likely to overclaim the privilege where there is no true trade secret.[167] Overclaiming becomes problematic and harmful to the administration of criminal justice because courts frequently deny defendants' discovery of a company's claimed trade secret.[168] This prevents defendants from gaining access to the inner workings of a company's technology—specifically the source code—which is needed for a defendant to meaningfully confront the witnesses that testify against him.[169]

Developers have already used the trade secret privilege to block defendants from gaining access to the source code of their

[162] Frank Pasquale, *Secret Algorithms Threaten the Rule of Law*, MIT TECH. REV. (June 1, 2017), https://www.technologyreview.com/2017/06/01/151447/secret-algorithms-threaten-the-rule-of-law/#:~:text=Sending%20people%20to%20jail%20because,program%20undermines%20our%20legal%20system.&text=Predicting%20and%20shaping%20what%20you,business%20for%20data%2Ddriven%20firms [https://perma.cc/KW8D-MVCW].

[163] *See* Cheng & Nunn, *supra* note 142.

[164] Wexler, *supra* note 136, at 1356.

[165] *Id.* at 1396.

[166] *Id.* at 1397.

[167] *Id.*

[168] *See id.* at 1397–98.

[169] *See* Chessman, *supra* note 116, at 183; U.S. CONST. amend. VI.

technologies.[170] For example, a California defendant was denied access to a forensic software's source code used to convict him of murder because the software developer claimed trade secret privilege.[171] The technology was a statistical tool that was used to calculate the likelihood that the defendant's DNA was in a sample from the crime scene.[172] A California trial court had ordered the developer to disclose the source code because the defendant's right to confront and cross-examine a witness would be denied without it.[173] However, the California Court of Appeal for the Second Circuit held for the developer concluding that the trade secret privilege applied in this criminal trial.[174]

Granting trade secret privilege in the criminal context can be problematic and raises concerns about the administration of justice. When evaluating whether to grant trade secret privilege to a company, a court's first consideration is whether the alleged trade secret is valid and whether ordering its disclosure would cause harm.[175]

Moreover, courts generally also weigh the risk of harm resulting from the disclosure against the need for the protected information.[176] Using this balancing test is problematic because it places a company's financial interests on the same level as a criminal defendant's life and liberty, which should be valued more heavily.[177] Further, the way that courts have generally applied this test in the criminal context suggests that intellectual property owners are prioritized over defendants in the criminal justice system.[178] Ultimately, defendants have a right to confront their accuser under the confrontation clause; using the trade secret privilege to prevent defendants from gaining access to the source code and inner workings of the technology that condemns them impedes the administration of justice.

Additionally, it is unnecessary for developers to invoke the trade secret privilege because there are already procedural safeguards in place to limit the defendant's access to protected information through

[170] *See* People v. Superior Ct. (*Chubbs*), No. B258569, 2015 WL 139069, at *3, *7, *9–10 (Cal. Ct. App. Jan. 9, 2015).

[171] *Id.*; Wexler, *supra* note 136, at 1358.

[172] *Chubbs*, 2015 WL 139069, at *1; Wexler, *supra* note 136, at 1358.

[173] *Chubbs*, 2015 WL 139069, at *4; Wexler, *supra* note 136, at 1358.

[174] *Chubbs*, 2015 WL 139069, at *10; Wexler, *supra* note 136, at 1358–59.

[175] Wexler, *supra* note 136, at 1396.

[176] *Id.*

[177] *Id.* at 1401–02 (discussing the "group value model" that Allan Lind and Tom Tyler developed in their book, E. ALLAN LIND & TOM R. TYLER, THE SOCIAL PSYCHOLOGY OF PROCEDURAL JUSTICE 228–40 (1998)).

[178] *Id.*

criminal discovery and subpoena procedures.[179] Courts can deny frivolous or abusive motions for discovery, and they can also grant protective orders to guard the trade secrets at issue.[180]

Ultimately, the rationale for the trade secret privilege—to encourage innovation and prevent unfair business practices—cannot justify a blanket trade secret privilege in the criminal justice system.[181] Criminal defendants are unlikely to be competitors of the private companies creating facial recognition technology; and therefore, the trade secret privilege should not be available to completely block defendants from access to the inner workings of the software.[182] However, it is worth noting that companies have an interest in protecting their information because defendants could be careless with it. It is foreseeable that a company's competitor in the marketplace could bribe a criminal defendant to disclose protected information that the defendant accesses during trial. Yet, given the seriousness of a criminal charge, on balance, criminal defendants who have been incriminated by evidence from facial recognition technology should have the right to challenge this evidence by accessing the source code and "looking under the hood" of these technologies, with possible protections for developers and their technology.

3. Challenging Facial Recognition Technology Evidence

If evidence from facial recognition technology is admitted into court, there are a variety of defenses that a defendant can invoke to bar the admission of the evidence. If granted access to the source code that provides insight into the inner workings of the technology, defendants can present arguments about the accuracy of the technology, the accuracy of the specific test that was run, and whether the test should have been run at all.

First, defendants can assert that the technology itself may be embedded with bias. On cross, a criminal defendant can expose issues in the way the algorithm was trained. These issues indicate the algorithm's poor performance with particular demographics and potentially an incorrect identification in the defendant's case.[183] As

[179] *Id.* at 1403.

[180] *Id.*

[181] *Id.* at 1356.

[182] *See id.* (explaining that the underlying rationales of trade secret law do not justify a privilege that protects trade secrets from people who will never be business competitors).

[183] *See NIST Study*, *supra* note 10; Hill, *supra* note 1.

mentioned above, studies have shown that facial recognition technology performs worse on Black subjects.[184]

Further, the photo that was used to run a facial recognition test may be challenged. As mentioned above,[185] facial recognition technology works best when a photo is taken head-on with good lighting and no movement.[186] However, when the technology is unleashed in uncontrolled circumstances, photos are taken from different angles with different lighting that could lead to less accurate results.[187] Moreover, a person's evolving appearance can lead to less accurate results due to newly grown facial hair, weight gain or loss, or aging.[188]

The use of facial recognition technology can also be challenged as an "unreasonable search" under the Fourth Amendment.[189] While protections against facial recognition searches have not yet been established in this context, recent Supreme Court jurisprudence suggests that certain protections exist against unfettered monitoring of citizens' whereabouts.[190] Facial recognition technology can be used to monitor the location of a person. Because this government action is particularly intrusive, the use of this technology could be challenged on Fourth Amendment grounds. In the 2012 *United States v. Jones* decision, the Court held that installing a GPS tracking device on an automobile and using it to track the vehicle's movements for an extended amount of time was a "search" under the Fourth Amendment.[191] Justice Alito wrote in his concurring opinion that "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[192] Further, in 2018, the Supreme Court held in *Carpenter v. United States* that accessing cell phone records for the purpose of obtaining the location of the device constituted a Fourth Amendment search and a probable-cause search warrant was needed to gain access

[184] *See NIST Study*, *supra* note 10.

[185] *See* discussion *supra* Section I.F.

[186] Hamann & Smith, *supra* note 13.

[187] *Id.*

[188] *Id.*

[189] U.S. CONST. amend. IV.

[190] *See* United States v. Jones, 565 U.S. 400, 404 (2012) (holding that installing a GPS tracking device on a vehicle and using it to track the vehicle's movements for an extended period of time constituted a search under the Fourth Amendment); Carpenter v. United States, 138 S. Ct. 2206, 2221, 2223 (2018) (holding that accessing historical cell phone records for purposes of obtaining the geolocation of the device constituted a search under the Fourth Amendment, and accessing them requires a probable-cause search warrant).

[191] 565 U.S. at 404.

[192] *Id.* at 430.

to such records.[193] Therefore, defendants can use existing case law to challenge law enforcement's use of facial recognition technology to monitor their location as a Fourth Amendment search requiring a probable-cause search warrant.[194]

III. SOLUTION

Based on the *Daubert* analysis in Part II,[195] this Note recommends that results from facial recognition technology should not be admitted into evidence based on the current state of the technology. Moreover, this Note recommends that Congress pass a law to grant defendants access to the software's source code if the software's results are admitted in their trials, with possible protections for the software developer's information.

A. Admissibility

The *Daubert* factors will guide federal judges' analysis when results from facial recognition technology are introduced in court. Results from facial recognition technology should not be admitted into evidence at trial because of the current lack of testing of facial recognition technology, the absence of meaningful peer review due to the proprietary nature of the technology, the difficulty in calculating an error rate, the shortage of industry standards, and the lack of meaningful general acceptance in the scientific community.[196] However, if standards or a testing protocol were established in this industry—as proposed in the Justice in Forensic Algorithms Act of 2019—then the *Daubert* analysis would evolve, and the evidence may be perceived as more reliable.[197] This would likely lead to admissions of evidence from

[193] 138 S. Ct. at 2221, 2223.

[194] *See Jones*, 565 U.S. at 404; *Carpenter*, 138 S. Ct. at 2221, 2223; Garvie et al., *supra* note 22.

[195] *See* discussion *supra* Section II.A.

[196] *See* discussion *supra* Section II.A.

[197] *See* H.R. 4368, 116th Cong. § 2(a) (2019). The proposed bill charges the NIST to establish Computation Forensic Algorithms Standards and a Computational Forensic Algorithms Testing Program that federal law enforcement must comply with when using forensic algorithms. *Id.* The NIST standards would include an assessment for potential for disparate impact on different demographics, requirements for software testing, requirements for developers' public disclosure of documentation about the software (including information about the development process and its training data), and requirements to provide defendants with reports that document the use and results of the forensic software program in their trials. *Id.* NIST's Testing Program would require testing in accordance with the NIST standards, that testing use realistic data sets that represent diverse racial and ethnic groups, and that the test results are published online with specifics about the software's performance on diverse populations. *Id.* § 2(d). The bill provides that

facial recognition technology. However, the current state of the industry suggests that results from facial recognition technology should not be admitted in federal court.

B. Contestability

Congress should adopt a law where criminal defendants are granted access to the results from forensic software used in their cases, access to the software itself, and access to the software's source code to challenge the evidence presented against them.[198] Further, Congress should allow developers to continue to claim trade secret privilege, but it should not block defendants from accessing the software. Instead, judges should make a case-by-case determination on how to best protect a developer's trade secret while also granting criminal defendants the right to access this critical source code.

For example, the proposed Justice in Forensic Algorithms Act of 2019 would protect defendants' access to the algorithms' source code by ensuring developers cannot assert a trade secret privilege to block defendants' access.[199] The bill creates a blanket rule that trade secret protections do not apply in criminal trials "when defendants would otherwise be entitled to obtain evidence" by amending the Federal Rules of Evidence.[200] Further, the proposed bill provides that defendants would receive a report on the software used in their cases and would be given access to the software so they can test it.[201] The extreme nature of this blanket ban on trade secret protections made the bill unlikely to pass.[202]

This Note supports the general spirit of this bill—ensuring that defendants obtain access to the software and its source code to challenge the evidence used against them. This proposed bill is problematic, however, because it disincentivizes innovation. If developers know that their trade secrets could be available to opposing parties in litigation at any time, the incentive to innovate and improve their products will be diminished. Their competitive advantage is eliminated if opposing parties gain full access to the developer's trade secrets and then disclose that information to competitors or to the public. Further, the proposal does not adequately weigh the intellectual property interests of the

evidence from forensic software would only be admissible in a criminal case if the software was submitted to the NIST testing program. *Id.* § 2(g)(1).

[198] *Cf.* Chessman, *supra* note 116, at 183; Imwinkelried, *supra* note 138, at 126–27.

[199] *See* H.R. 4368, 116th Cong. (2019).

[200] *Id.* § 2(b).

[201] Takano, *supra* note 74.

[202] *See generally* H.R. 4368, 116th Cong. (2019).

companies. Instead of a blanket rule against a trade secret privilege, a more nuanced solution would better balance the competing interests at issue. This Note proposes a middle-ground approach: developers may invoke the trade secret privilege in criminal cases, but they cannot categorically block the defendant's access to the software.

In practice, a court would first issue an order specifying the conditions under which the defendant can have access to the company's software and documentation. The company would be responsible for enforcing the court-ordered protections for its software. After giving the defendant access to this information, it would be up to defendant's counsel to closely scrutinize the software and its inner workings. Defendant's counsel may consider hiring an expert to assist in understanding the technology's source code. While this may be costly for the defendant, this solution provides criminal defendants with an opportunity to meaningfully confront their accusers.

This approach would leave the door open for judges to provide protection for the developer. For instance, after giving defendants access to the software's source code, the judge could decide that its disclosure is subject to a protective order.[203] For example, courts have required disclosure subject to protective orders with varying constraints: the experts granted access are subject to vetting; the experts sign a declaration to acknowledge their obligation not to circulate the protected information; the experts are allowed to study the information exclusively in secure areas; and the experts have to conduct their analysis on protected computers.[204] These types of provisions ensure protection for the developer and also give the defendant access to the software so the defendant can meaningfully challenge the evidence presented against him. This solution does not always require protective orders because it is possible that, in some cases, the threat of private information disclosure is so low that it does not outweigh the costs associated with enforcing a protective order. As demonstrated, a case-by-case approach is the best solution for deciding what protections are granted to developers that avoid treading on a defendant's right to confrontation.

IV. CONCLUSION

This Note cautions against admitting results from facial recognition technology into evidence at trial based on the current infancy and bias of the technology. Further, if the evidence is admitted,

[203] *See* Imwinkelried, *supra* note 138, at 127.

[204] *See id.*

defendants should have access to the software's source code to meaningfully challenge the evidence presented against them under the confrontation clause. This Note recognizes the developers' interest in protecting trade secrets and argues that judges should make case-by-case determinations about how to protect developers' information without blocking defendants' access to the software.

Because of the current bias of facial recognition software and its disparate accuracy in identifying different demographics, it is important to critically analyze the state of the technology and the industry before allowing it to be admitted into evidence at trial. This Note presents a call to action to examine law enforcement's use of facial recognition technology and to prevent unreliable uses from incriminating defendants without an opportunity for these defendants to exercise their constitutional right to confront the algorithm that accuses them.

Gabrielle M. Haddad[*]

[*] J.D. Candidate, Vanderbilt University Law School, 2022; B.A., Furman University, 2019. The Author would like to thank Professor Christopher Slobogin and Professor Edward K. Cheng for their guidance which facilitated the research on facial recognition technology that served as the foundation of this Note. The board and staff of the *Vanderbilt Journal of Entertainment and Technology Law* deserve special recognition for their thoughtful feedback and attention to detail that brought this Note to publication. The Author would also like to thank her family, friends, and mentors who encouraged her while she was pursuing a legal education and writing this Note during the COVID-19 Pandemic. The Author wants to especially thank her mother, Mary Haddad, who has always emphasized the importance of working toward excellence and positively impacting others along the way.