



© Viks_jin | AdobeStock

Challenging Facial Recognition Software in Criminal Court

While the idea of police officers sitting around computers inputting pictures into facial recognition software may sound futuristic, it is already happening. If an image of a perpetrator exists on a cellphone camera, video surveillance, body camera footage, social media or any other recording, law enforcement can use facial recognition to attempt to link the person in the photo to an identity.

Federal agencies and high profile investigations are not the only places where facial recognition software (“FRS”) is being used. State and local law enforcement agencies employ FRS in investigations that range from serious to relatively mundane. FRS has been used to pinpoint suspects in cases as routine as drug sales,¹ petty theft,² robbery, and identity theft.³

How Does Facial Recognition Work?

FRS works by comparing faces in two photos and making a determination about whether it is the same person in each photo.⁴ In criminal cases the police

input a “probe photo” of the person believed to be the true perpetrator into the software. The probe photo can come from any source that records photos or video. The software compares the probe photo to a database of images of known people. In some jurisdictions the database of known people is limited to mug shots, but others include civilian photos from the Department of Motor Vehicles.⁵

In the criminal context the software has two different functions — face verification and face identification.⁶ In face verification, police use FRS to confirm that apprehended suspects are who they say they are. In face identification, FRS is used to link a photo of an unknown person to an identity. The technology is not yet advanced enough to “match” a photo of an unknown person to an identity. Instead, the software produces a number of “possible match candidates.”⁷ A police officer (sometimes with special training and sometimes not) reviews the possible matches and compares them to the probe photo. It is that person, not a computer, who makes the final decision about the identity of the person in the probe photo.⁸

In limited circumstances face verification is used as evidence in court.⁹ Face identification is not. Because the technology cannot actually “match” a photo to an identity and has other accuracy problems, it is not accepted as scientifically reliable (though that may change in the future).¹⁰ Right now, face identification software is used to develop investigatory leads. It is not evidence that is admissible in court.¹¹ Consequently, the use of FRS is not always disclosed to the defense. It is this type of FRS case — face identification — that defense attorneys should be looking for and challenging.

BY KAITLIN JACKSON

Facial recognition software has limitations.

It is not necessary to deeply understand the technology to raise a legal challenge to its use. But it is important that defense attorneys are familiar with its basic limitations. The overall accuracy of FRS is disputed.¹² However, for reference, fingerprint recognition is broadly accepted as a more accurate forensic discipline than face recognition.¹³ The state of the art FRS run on a curated set of images only performs in the same range as trained human facial examiners.¹⁴ It is hard to say what this means in terms of accuracy in the field because, in the real world, conditions are often not ideal and law enforcement may not be using state of the art programs. Further, no rules govern what types of edits law enforcement is permitted to make to photos before running them through FRS.¹⁵

The quality of the software's output is directly related to the quality of the probe photo. When the quality of the probe photo is high, the software will produce better results than when the quality of the probe photo is low.¹⁶ Similarly, to perform optimally, FRS programs prefer that the images being compared have a similar orientation (i.e., both faces should be looking at the camera).¹⁷ Because the probe photos in criminal cases come from sources like surveillance video, the probe photos are often not front-facing high resolution images.¹⁸ In order to address the problem of low quality images, some law enforcement agencies permit substantial editing of probe photos. These edits can be as extreme as replacing facial features from the probe photo with features from stock images (such as replacing closed eyes with open ones, or an open mouth with a closed one).¹⁹ In one case in New York, law enforcement went so far as to substitute a high quality image of Woody Harrelson for a low quality probe photo of a perpetrator who police thought looked like Woody Harrelson.²⁰ Another technique law enforcement officers use on probe photos is reorientation of the face so that it is front-facing by "mirroring" the portion of the face that is visible, and digitally approximating what the other side of the face would look like.²¹ The more editing that is done to a probe photos, the less reliable the results will be.

Even when the original probe photos come in the form that FRS prefers, the software performs consistently better for certain populations than for others. For example, facial recognition algorithms are less accurate at identifying women, young people, and African

Americans.²² The accuracy of FRS drops off substantially for certain populations even in tasks simpler than face recognition. For example, FRS misclassifies the sex of dark-skinned women as often as a third of the time.²³

Another challenge for FRS programs is that faces change, which is not true for fingerprints or DNA. Glasses, makeup, expression, and hairstyle can all fundamentally affect the way a face looks.²⁴ While human eyes can look at pictures of someone facing different directions, with varying expressions or at different ages, and effortlessly recognize that it is the same person, machines notoriously struggle with that task.²⁵

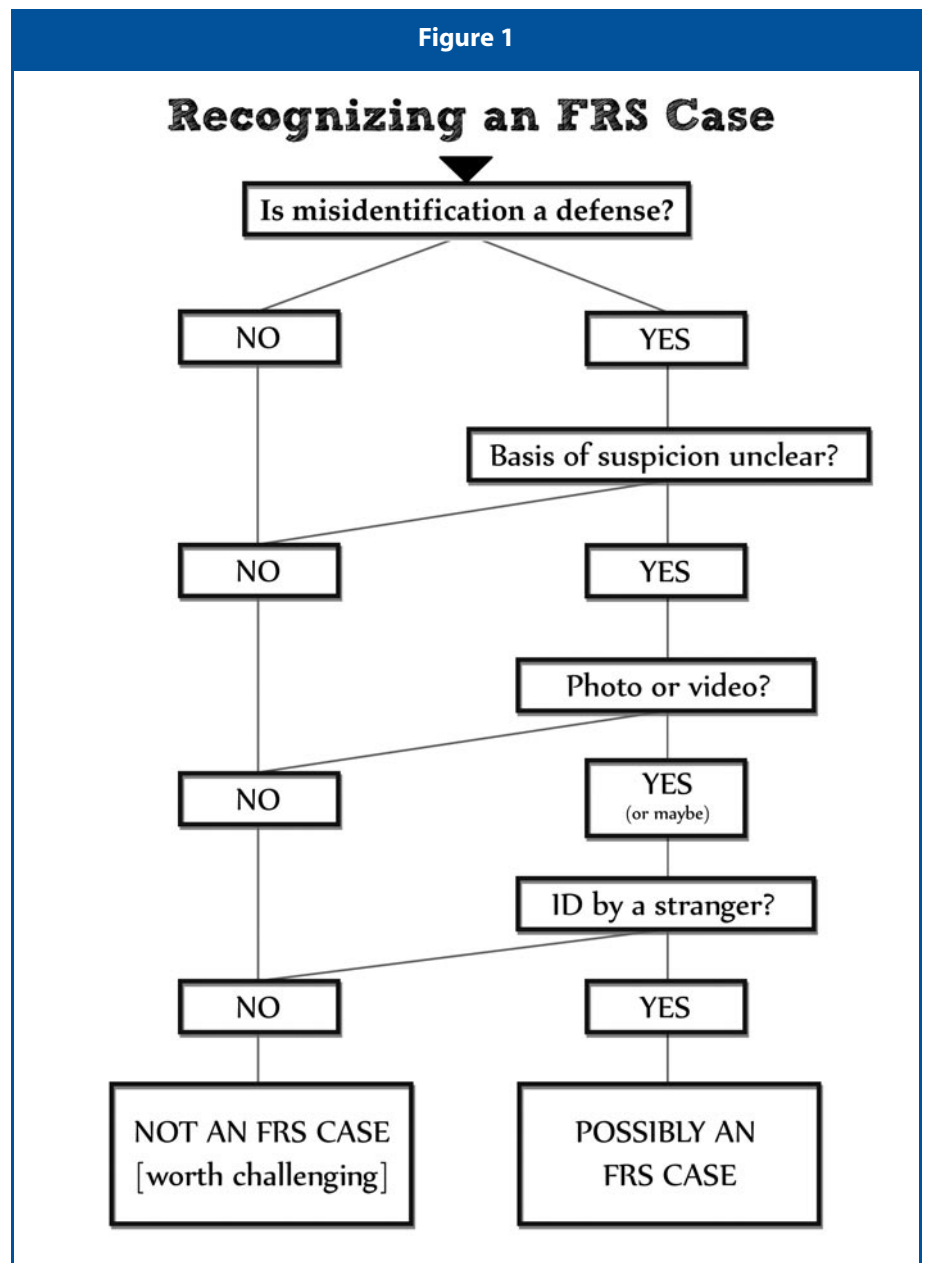
Courts are sometimes deferential to evidence that comes from computers. It is important for defense attorneys to be aware that while machines are incredibly

good at some tasks, there are categories of tasks for which machines are less proficient than humans. Recognizing faces is a mix of the types of tasks that machines are traditionally good at, and the types of tasks that machines struggle with. For example, computers can compare huge databases of faces at a speed no human can equal. On the other hand, humans can easily recognize a person in a video who is moving, a task even the most advanced computers do not do well.²⁶

How Do Defense Lawyers Recognize a Facial Recognition Case?

A more appropriate title for this section is "how to recognize cases where facial recognition was used in a way that can be challenged in criminal

Figure 1



court.” FRS is used in myriad ways, many of which — like face verification — are ripe for *civil* legal challenges. A narrower set of cases lend themselves to criminal challenges. Those are cases where there is a viable argument that the use of facial recognition contributed to an arrest without probable cause or an arrest of the wrong person. These are the cases defense lawyers should try to isolate.

The first hurdle to an effective challenge is recognizing the cases in which FRS was used. Because police use FRS exclusively as an investigative tool in the face identification context, the state might not disclose its use to the defense.

FRS is used (and concealed) this way: Police use FRS to zero in on a suspect. Once they have a suspect, law enforcement does additional investigation to collect other incriminating evidence (sometimes compelling and sometimes not) against the suspect. Often, but not always, the additional investigation will include putting the suspect in an identification procedure for a human witness to identify.

The police and prosecution then rely on the *other* incriminating evidence when drafting the charging documents. By the time the defense attorney enters her notice of appearance, the use of FRS

may be so deeply buried that, unless the attorney knows to look for it, she may never discover it was used at all.

There is no guaranteed test to isolate cases in which the police used FRS. But there are features that defense attorneys can look for in their cases to spot likely candidates. Figure 1 contains a list of four questions. If the answer is yes to all of them, the attorney should take steps to determine whether FRS played a role in the client’s arrest.

Is the defense misidentification?

The first question an attorney should ask is whether there is a colorable misidentification defense. A feature of any criminal challenge to the use of FRS will be the argument that the software selected the wrong person. The defense can only make that argument if a misidentification defense is viable.

If a misidentification defense is not possible, FRS may still have been used. However, those are not the FRS cases defense attorneys need to pinpoint. The goal is to find cases in which a challenge to FRS helps the lawyer craft an argument for innocence or suppression. And those are cases where the defense attorney can argue that the software made a mistake that led to a false arrest or an arrest without probable cause.²⁷

Another way to frame this question is, “Was there a lag in time between the incident and the arrest?” A time gap is critical. If the client was apprehended at the scene of the crime, it is unlikely that FRS was a factor leading to the arrest. On the other hand, if the client was arrested days or weeks after the incident, it is possible that FRS played a role in the decision to arrest the client.

Once an attorney is satisfied that a misidentification defense is available, she should consider the next factor.

Is it unclear why the client was suspected of this crime?

The second task is determining why the client was initially suspected of committing the crime. If the initial basis of suspicion is not obvious from the charging documents, it is possible that FRS played a role.

The question the attorney should be asking is not about the sum total of the evidence — an FRS pairing could be made first, and additional evidence against the client could be collected after. Rather, the issue is, “What gave rise to the initial suspicion?” For example, if the client was identified by an eyewitness, the attorney should be asking, “What led law enforcement to put the

client in an identification procedure?” If the criminal activity was caught on surveillance and the prosecution claims the surveillance shows the client, then the question becomes, “Who watched the surveillance and decided that the client was the person in the video?” If the police were actively looking for the client prior to his arrest, why?

In many cases, the initial basis for suspicion will be obvious. If the defendant was arrested because a 911 caller provided his address, for example, FRS most likely is not the reason the client was a suspect. If the client’s DNA or fingerprints were left at the scene, it is also unlikely that FRS was the source of the initial suspicion. In other cases, it will be less obvious how law enforcement connected the criminal activity to the client, and those are the cases that attorneys should be looking for.

If the reason the police initially suspected the client is not apparent to the attorney, she should move to the next factor.

Is there a photo or video of the incident?

A recording of a face is a prerequisite for the use of FRS. If there is no photo or video connected to the incident, then FRS was not used to develop a suspect.

Sometimes an attorney will know for certain that there is a recording. In other cases, an attorney may not know whether photo or video exists. Particularly in the early stages of a case, an attorney may be unsure whether video surveillance, cellphone recordings, or body camera footage exists. To the extent the attorney knows that there is a recording (and the above factors are present as well), the attorney also knows that there is a possibility FRS was used. Likewise, if the attorney is relatively certain that a recording was not produced in connection with an incident, she knows FRS was not a factor in the decision to arrest his client.

Once the attorney has determined that photo or video connected to the incident does (or may) exist, she should move on to the last factor.

Was there an identification by a stranger eyewitness?

It is a well-established principle of law that when an eyewitness knows the defendant well, there is no prejudice to the defendant if the police hold a suggestive identification procedure.²⁸ The theory is that no amount of suggestiveness would cause someone to



National Advocacy Calls on Developing Legislation (NACDL)

Monica L. Reid hosts this recurrent conference call series to inform advocates of legislation and litigation that impact criminal justice issues. The calls generally feature a presentation by an expert and a question and answer segment with listeners.

To listen please visit
NACDL.org/scjnadvocacycalls

07132018

misidentify a good friend, for example. The same principle applies in FRS cases. If the defendant was identified by someone who knows him well, there is no credible argument available that FRS influenced that person to make a misidentification.

Consequently, the final question that the attorney should be asking is, “How does the state intend to prove identity?” The cases the defense is interested in challenging are the ones where FRS was used by law enforcement because the identity of the perpetrator was initially a mystery. Typically, in these cases, the defendant will be identified at trial by a person who does not know him well.

Sometimes that person is a civilian. But sometimes that person will be a police officer. In a Florida case, an undercover officer took a cellphone picture during a drug sale. The officer sent the photo to be run through facial recognition software. Later the officer positively identified the suspect developed by the software in a single photo identification procedure.²⁹

Not every case includes a pretrial identification procedure. But the state does have to prove identity in every case. When considering this fourth factor, the attorney should consider whether there is a preexisting relationship between the defendant and the person who will testify about the defendant’s identity at trial. If there is not (and the other factors are present), it is possible that FRS played a role.

If the answer to all these questions is “yes,” then the attorney should take steps to determine whether FRS played a role in the investigation. The first and simplest action step an attorney can take is to call the prosecution and ask. If the defense attorney learns that law enforcement used FRS, or alternatively, if the attorney cannot get an answer, she should file a discovery demand. And finally, if that is unsuccessful, the attorney should file a motion to compel, specifically requesting information about the use or nonuse of FRS.

If the answer to any of the above questions is “no,” it is improbable that the police used FRS, although it is possible. However, if it was used, it is unlikely it was used in a way that lends itself to a fruitful challenge in criminal court. Nevertheless, this is a new technology, and there may be future uses and challenges that are not currently foreseeable. Consequently, if the attorney suspects FRS may have played a role, it is wise to take additional steps to confirm or deny that suspicion.

Why Is Facial Recognition Difficult to Challenge?

Once a defense attorney is confident that police used FRS, the next step is developing a plan to challenge it in court. That is not a straightforward task. FRS is difficult to challenge in the criminal context for two primary reasons. First, there is no legal mechanism to contest the defendant’s presence in an identification procedure. Second, there is no legal mechanism to contest forensic practices that will not be introduced by either party at trial. Defense attorneys must contend with the fact that the current legal framework is ill equipped to handle the unique problems posed by FRS. It is only after an attorney understands and accepts these two complications that she can start to work around them.


There is no legal mechanism to challenge the defendant’s presence in an identification procedure.

Often FRS is used to select suspects for identification procedures. Those can be live lineups, photo lineups, or even single photo showups. If the software is working correctly, the suspect picked by the program should look very much like the true perpetrator (whether it is the true perpetrator or not). As a result, one would expect a reasonably high rate of human eyewitnesses confirming the software’s decisions.



The initial instinct of many attorneys is to view this process as two separate identification procedures — one by a machine and one by a human — and seek to suppress both. While the instinct is understandable, this is not a useful framework to start from. The identification by the human eyewitness is evidence that could potentially come in at trial. The selection by the software is not.

Someday that will change. And when the day comes, defense attorneys should seek to suppress machine identifications. But until then, arguing that FRS is making an identification does not benefit the defense because there is no evidence to move to suppress.

Instead, defense attorneys must attack the identification by the human eyewitness. But that is a challenging task. A common (but misguided) strategy is to argue that the defendant should not have been placed in an identification procedure based on an FRS pairing. This argument has no legal merit. The police do not need probable cause to put a suspect in an identification procedure. They do not need reasonable suspicion or any other quantum of evidence to be



Help your Clients
Break Free / Stay Free
with
WINGMAN®
When client’s cravings occur
solutions are there 24/7
Help clients make better
decisions, stay
on track one day at a time
WINGMAN
Will help battle addiction



See WINGMAN in Action
at NACDL Philadelphia
Meeting 7/31 - 8/3/19
go to: alexaforaddiction.com

permitted to use a defendant’s likeness in an identification procedure.³⁰

The law (as it currently stands) permits law enforcement to use any number of unreliable methods to select people for identification procedures. The police could rely on a psychic, take tips from unreliable informants, or pull photos out of mug shot books at random. All of those methods would pass constitutional muster because a defendant has no legal right to keep his likeness out of an identification procedure.³¹ The fact that FRS is widely considered too unreliable to be admitted as evidence in court does not give the defense an avenue to argue that suspects selected by FRS should not be put in identification procedures.³²

Any attack on FRS must take that principle into account. One argument that attorneys can make is this: the inclusion of a suspect selected by FRS *unreasonably increased the chance of eyewitness misidentification*. Eyewitness are likely to positively identify machine-selected look-alikes, regardless of whether they are the true perpetrator. Consequently, without indicia that FRS is scientifically reliable, the resulting eyewitness identification should be suppressed. That is not the only argument an attorney could advance. As long as

the attorney is cognizant of the fact that she cannot legally challenge her client’s presence in the identification procedure, there is room for creativity.

There is no legal mechanism to challenge forensic practices that will not be introduced at trial.

The second obstacle to contesting FRS is that there is no framework in place to contest the reliability of forensics that neither party intends to introduce at trial. Typically, when the defense disputes the validity of a forensic method, they ask for a *Daubert*, *Frye*, or similar state-specific hearing (depending on the jurisdiction).³³ At those hearings the prosecution bears the burden of showing that the forensic evidence is admissible. The standard for admissibility varies, but always includes some showing of scientific reliability. If the prosecution cannot meet its burden, the remedy is exclusion of the forensic evidence.

That remedy is not available in FRS cases because prosecutors are not seeking to introduce FRS evidence in trials — *yet*. Consequently, if the defense requests a *Daubert*, *Frye* or similar hearing, the prosecution will likely respond that it does not intend to introduce FRS evidence at trial; and

the court is likely to deny the request.³⁴

This will not be a problem forever. Eventually FRS technology will advance to a point where the state seeks to introduce machine identifications in trials. When that happens, the time will be ripe to request *Daubert* and *Frye* hearings. Until then, however, attorneys must be cognizant of the fact that this technology operates in a way that shields it from traditional methods of judicial review.

In order to challenge the underlying science, attorneys must be innovative. Likely this will require formulating a new type of hearing. One possible framing is this: eyewitnesses are likely to confirm the selections made by FRS because suspects selected by FRS will *always* look like the true perpetrator. Without testing the scientific reliability of FRS, it is not possible to tell whether FRS increases the number of true positive identifications or simply closes out cases by increasing the number of false positives. This danger is even more acute when other features of unreliability are present, such as a cross-racial identification. Therefore, the court should test the scientific reliability of FRS at a hearing. If the court determines that the technology is unreliable, then the remedy would be the suppression of the eyewitness identification (not exclusion of the forensic evidence).

That is only one possible challenge. As long as attorneys accept that the current mechanisms for challenging forensic evidence are not available in the FRS context, there are many ways an attorney could seek to attack the reliability of the program.

What Relief Should Defense Counsel Request?

No method to oppose FRS guarantees success in court. Courts have denied discovery requests,³⁵ disagreed about what constitutes *Brady* material,³⁶ and declined to grant suppression. In other cases, when courts have granted relief, the prosecution has moved to dismiss cases or extended new offers, so that the granted relief was never realized.

While there is no comprehensive checklist of remedies that attorneys should seek (or ways to frame those requests), there are some forms of relief that attorneys should be requesting in every FRS case: discovery, *Brady* material, and suppression of identifications (related to FRS).

Request discovery early and often.

Attorneys should ask for two broad types of discovery in FRS cases: (1) discovery related to the FRS search, and (2) discovery related to the FRS program. Figure 2 does not contain an exclusive list of information to request. The items listed are merely a jumping off point.

Ask for discovery related to the FRS search.

The first type of discovery that attorneys should seek is discovery related to the FRS search that was done in the case. Different FRS programs will produce different paperwork. However, when a search is run, all programs document the results. Remember, FRS always produces multiple candidate suspects as opposed to a single “match.” The software assigns a confidence score to each possible match candidate.³⁷ Attorneys should request that information in its entirety. The list of candidates and confidence scores is not only discovery that should be turned over, but also arguably exculpatory material (the next section of this article contains suggestions for framing this request through the lens of *Brady*).

Attorneys should also request disclosure of any editing that was done to the probe photo. It is common for FRS programs to use a process called normalization to electronically alter faces in order to achieve better results.³⁸ Sometimes this is done by reorienting faces so that they are front-facing or

Figure 2

FRS SEARCH DISCOVERY	FRS SOFTWARE DISCOVERY
<p style="text-align: center;"><u>PHOTOS</u></p> <ul style="list-style-type: none"> •Original probe photo (and all edited versions) •Original database photo of client (and all edited versions) •Other photos run through FRS in this case, regardless of whether a pairing was made (and all edited versions) •Photos of all possible match candidates 	<p style="text-align: center;"><u>SOFTWARE</u></p> <ul style="list-style-type: none"> •Program •Manufacturer •User Manual •Algorithm(s) and source codes •Error rates •Validation studies •Calibration or proficiency tests •Crash reports, corrective actions, and software updates •Parameters selected (Example: Was the software set to look for photos that were 80% matches to the probe photo or 95% matches?)
<p style="text-align: center;"><u>CANDIDATE LIST</u></p> <ul style="list-style-type: none"> •Confidence scores for all possible match candidates •Name of person who selected client •All notes made by that person •Results of any proficiency testing for that person 	<p style="text-align: center;"><u>DATABASE</u></p> <ul style="list-style-type: none"> •Where do database photos come from? •How often are photos removed? •Who has access to the database? •Are there written instructions for maintaining the database?

changing contrast. Law enforcement also has the ability to manually alter probe photos, sometimes making minor changes, and sometimes making extreme changes. Any changes made to the probe photo could have made the software's output less reliable, so it is critical that attorneys ask for changes made by the software and manual changes made by law enforcement.

Finally, attorneys should inquire into whether more than one probe photo was run through FRS. Particularly when the probe photo is a still shot from a video capture, there is no reason to believe that law enforcement is only inputting a single image. If law enforcement officers put more than one image through FRS, it raises these questions: What were the results of the other FRS runs? Did the software return different results? If so, an attorney could potentially incorporate that information into a misidentification defense. There may be cases where it is part of the defense strategy to introduce FRS results at trial even though the prosecution will not. Attorneys will only be able to make that call, however, if they have discovery.

Seek discovery related to the FRS program.

The other type of discovery that attorneys should be seeking is information about how FRS functions. In order to expose problems with FRS, attorneys need more complete information about how the software works.

In that vein, the defense should request broad disclosure. At the same time, attorneys should anticipate that they will not get everything they request. For example, the name of the program and the user manual are things that law enforcement almost certainly has, and could turn over. On the other hand, it is doubtful that law enforcement has access to FRS algorithms. The manufacturers will almost certainly fight requests to share their intellectual property, and judges may find that the algorithms are proprietary information to which the defense is not entitled.³⁹ The "trade secrets" barrier has prevented defense attorneys from getting access to algorithms for a variety of forensic software programs, most notably DNA software.⁴⁰ Some attorneys have argued that the Sixth Amendment right to confront one's accuser mandates disclosure of the program's algorithm to the defense. That argument has had limited success with DNA software.⁴¹ It remains to be seen whether it will have better results in the FRS context.

The best course of action is to request broad disclosure, but also prepare a more limited discovery demand should the broad request be denied. If the court finds that the defense is not entitled to data that contains trade secrets, the defense can use that distinction to argue that the opposite is also true: the defense is entitled to program data that *does not* contain trade secrets (like error rates and validation studies).

File Brady demands in every case.

In *Brady v. Maryland* the U.S. Supreme Court held that prosecutors must disclose evidence to the defense if it is exculpatory and material.⁴² Two pieces of discovery in FRS cases arguably fall into this category: (1) the list of other possible match candidates, and (2) rankings assigned to those suspects (called confidence scores). Attorneys can strengthen their discovery requests by framing this portion of the request as a *Brady* demand.

One tactic attorneys can use to persuade courts that candidate lists and confidence scores are *Brady* material is to draw analogies between FRS and human eyewitnesses. Imagine this scenario:

An eyewitness viewing a lineup points to the defendant and a filler and says, "It was one of these two people."

If a human identified two people as the possible perpetrator, the prosecution would (most likely) be obligated to disclose that information.⁴³ The analogy to be drawn is that FRS is doing essentially that — identifying multiple people. If it is *Brady* information when a human identifies multiple suspects, it should be *Brady* information when a machine does.

Next, imagine this scenario:

An eyewitness viewing a photo pack selects the defendant and says, "I think that was the person I saw, but I can't be sure. It could be someone else."

The prosecution would (most likely) have to disclose the eyewitness's statement about the lack of certainty to the defense.⁴⁴ This is analogous to FRS confidence scores. The software tells law enforcement in every case that it is uncertain that the defendant is the perpetrator. The software even assigns a value to that uncertainty. If the lack of certainty is exculpatory when it comes from a human eyewitness, the same should be true when it comes from a machine.

FEDERAL PRISON AUTHORITY

(214) 431-2032

<https://www.FederalPrisonAuthority.com>

federalprisonauthoritybop@gmail.com

WE OFFER THE FOLLOWING SERVICES:

- FIRST STEP ACT ANALYSIS
- PRE-TRIAL/PSR INTERVIEW
- PSR REVIEW/ REVIEW OBJECTIONS
- SECURITY & CLASSIFICATION ASSESSMENT
- SENTENCE COMPUTATION
- INITIAL DESIGNATION
- PROGRAMS RDAP/SEX OFFENDER
- REDESIGNATION TRANSFERS
- ADMINISTRATIVE REMEDIES
- RRC ASSESSMENT/SECOND CHANCE ACT



BRUCE CAMERON MS, LPC-S, LSOTP-S & JOSE A. SANTANA JD

Lawyers for the prosecution may argue that they are under no obligation to disclose the results of the FRS search because they do not intend to introduce them at trial. However, while *Brady* is applied in a famously inconsistent manner, most jurisdictions mandate disclosure of exculpatory information that could lead to admissible evidence (even if the exculpatory information is not admissible in its current form).⁴⁵

When writing a *Brady* demand, keep in mind that while there is precious little case law about FRS, there is a wealth of case law about disclosure obligations in the eyewitness identification context. Analogizing the two provides a road map for making arguments about discovery in FRS cases.

Move to suppress identification testimony.

The most elusive (but most useful) remedy an attorney can ask for in an FRS case is suppression of an eyewitness identification. Remember, in the common FRS case the identification comes about this way: the defendant is selected by FRS, put in an identification procedure, and then identified by an eyewitness. Attorneys should be crafting arguments to suppress those identifications — but that takes creativity.

Trial courts have a mandate to limit the admission of misidentifications.⁴⁶ Trial courts typically follow that directive by holding pretrial hearings to evaluate the suggestiveness of an identification procedure.⁴⁷ If a trial court finds that law enforcement held an identification procedure that was so unnecessarily suggestive that an irreparable likelihood of misidentification exists, the identification cannot come in at trial.⁴⁸ Typically, when courts make such a finding, it is because law enforcement suggested to the eyewitness whom to pick.

In the case of FRS, the concern over misidentification is not related to law enforcement sending (intentional or unintentional) signals to the eyewitness. Rather, the concern is that FRS selects suspects based solely on the single factor most likely to result in a positive identification — facial features that are similar to the perpetrator's. As a result, FRS is likely to increase all positive identifications, both true positives and false positives.

Typical suppression arguments are (usually) ill fitted to address the risk of misidentifications resulting from the use of FRS. Luckily, courts have broad discretion to rule on the admissibility of evidence pretrial. So attorneys can put forth a different argument. One possible argument is this: the eyewitness identification of a suspect selected by FRS should be suppressed if the software cannot be shown to meet accepted scientific standards of reliability.

Before delving more deeply into that line of reasoning, it is important to note that there is one set of circumstances in which FRS does increase traditional suggestiveness: cases where the eyewitness knows that a suspect in the identification procedure was selected by FRS. That information is suggestive, and in that scenario, attorneys can incorporate traditional suggestiveness arguments into the suppression litigation they are already doing.

Ideas for structuring arguments about suggestiveness when the eyewitness is aware that FRS was used, and ideas for putting forth arguments that FRS increases the risk of misidentifications, are laid out more fully below.

Asking an eyewitness to identify a suspect the eyewitness knows was previously selected by FRS is suggestive.

Some eyewitnesses will know that a suspect they are being shown was selected by facial recognition. The knowledge that FRS was involved in the investigation may give an eyewitness a false belief that the true perpetrator *must* be present

in the procedure. While that implication has rarely been found to be impermissibly suggestive in isolation, in combination with other suggestive factors, courts have suppressed identifications.⁴⁹

When the eyewitness is a police officer, the officer will often know if FRS was used. A compounding problem in FRS cases with police eyewitnesses is that single photo identifications are more common. Single photo identification procedures are widely considered suggestive.⁵⁰ In combination there is a nontrivial risk that an eyewitness will echo the software's decision even if it conflicts with his own memory.

Sometimes civilian eyewitnesses will also be aware that law enforcement used FRS. Police may inadvertently mention it. Improper influence can be just as easily generated by sloppy behaviors as intentionally suggestive ones. In a case in New York, a police officer collecting surveillance told an eyewitness that he planned to run the video through FRS. A few days later the officer held a single photo identification with the civilian.⁵¹ It may not have occurred to the officer that discussing FRS had the potential to improperly influence the later identification procedure. Regardless, it did.

Where possible, send investigators to talk to eyewitnesses and inquire about what information they had in FRS cases prior to the identification procedure. When the eyewitness is a police officer, attorneys should assume that the officer eyewitness knew if FRS was used. If the eyewitness was aware that police used FRS (prior to selecting the defendant), the defense should argue that the procedure was unreasonably suggestive.

Absent a showing of scientific reliability, the increased risk of misidentification from the use of FRS is unreasonably high.

Fear about misidentifications led the Supreme Court to create an exclusionary rule for suggestive identifications.⁵² The animating concern in this area is not fairness; it is innocence.⁵³ For example, there is no blanket prohibition on suggestive identification procedures, just those that are so suggestive that there is irreparable risk of misidentification.⁵⁴ Plainly, the issue that the court is regulating is limiting the admission of misidentifications.

Theoretically, it is possible to have an identification procedure that, without being suggestive, is likely to cause misidentifications. If the risk of misidentification is unacceptably high, the courts *should* still suppress identi-

fication testimony — even absent suggestiveness. There is an argument that facial recognition does just that: increases the likelihood of misidentification, but evades judicial review because it is not traditionally “suggestive.”

Why? Stranger eyewitnesses are unlikely to be good at distinguishing between the true perpetrator and a look-alike. It stands to reason that FRS increases the rate of all positive identifications — both false positives and true positives. How much the look-alike problem increases the risk of misidentification depends on how often the software selects the wrong person.

In order to determine whether using FRS increases the risk of misidentification, the court would need to test the scientific validity of FRS at a hearing. At the end of the hearing, if the court found FRS to be scientifically reliable, then the eyewitness identification should be admitted. In that scenario there is no reason for the court to fear that FRS is likely to increase the risk of misidentification. On the other hand, the outcome of the hearing might be that FRS is unreliable. If FRS frequently selects look-alikes instead of the true perpetrator, then a real danger of misidentification exists in presenting those look-alikes to human eyewitnesses for identification. In that scenario, the remedy the defense should seek is suppression of the eyewitness identification because the risk of misidentification is so great.

The shape of this argument is a bit unorthodox. However, because of the unique challenges presented by FRS, any argument for suppression will have to be. One way to make the request for suppression more accessible is to analogize FRS to other forensic practices. For example, in many jurisdictions identifications by witnesses who have had their recollections “enhanced” using hypnosis are inadmissible.⁵⁵ This is an example of a forensic practice that is so likely to increase misidentifications that eyewitnesses who are exposed to it may not give identification testimony, even if the prosecution does not seek to admit evidence about the forensic practice. The argument that attorneys should advance in FRS cases is parallel — that a forensic method used prior to the identification procedure rendered the identification unreliable (and hopefully inadmissible).

What Is the Takeaway?

FRS is a new frontier in criminal courts. The legal protections that exist

to prevent defendants from being prosecuted through bad forensics and unreliable identifications are ill suited to address FRS. The defense bar has a responsibility to understand why traditional legal mechanisms will not work in this context and press the law to keep pace with the changing technology. Asking for novel remedies can feel daunting. However, every suppression remedy that is available only exists because some defense lawyer was the first to ask for it.

© 2019, National Association of Criminal Defense Lawyers. All rights reserved.

Notes

1. *Lynch v. State*, 260 So.3d 1166 (Fla. Dist. Ct. App. 2018), *reh'g denied* (Jan. 17, 2019).

2. Ben Fox Rubin, *Facial Recognition Overkill: How Deputies Cracked a \$12 Shoplifting Case*, CNET, Mar. 19, 2019, <https://www.cnet.com/news/facial-recognition-overkill-how-deputies-solved-a-12-shoplifting-case>.

3. *United States v. Badiane*, 725 F. App'x 828 (11th Cir. 2018).

4. CLARE GARVIE, ALVARO BEDOYA & JONATHAN FRANKLE, *THE PERPETUAL LINEUP: UNREGULATED POLICE FACE RECOGNITION IN AMERICA*, GEORGETOWN CENTER ON PRIVACY AND THE LAW (2016), <https://www.perpetuallineup.org>.

5. GARVIE ET AL., *supra* note 4.

6. *Id.*

7. *Id.*

8. *Id.*

9. See, e.g., *Badiane*, 725 F. App'x 828; *United States v. Gibson*, No. 8:00-CR-442-T-27AEP, 2016 WL 845272, at 2 (M.D. Fla. Mar. 4, 2016), *aff'd sub nom. United States v. Lazzara*, 709 F. App'x 578 (11th Cir. 2017).

10. See *People v. Collins*, 15 N.Y.S.3d 564, 576 (N.Y. Sup. Ct. 2015) ("The products of polygraph technology and of facial recognition technology similarly can sometimes have value, but evidence produced by those technologies is not generally accepted as reliable by the relevant scientific communities and so cannot be admitted in trials.").

11. *Id.*

12. Drew Harwell, *Amazon Facial-Identification Software Used by Police Falls Short on Tests for Accuracy and Bias, New Research Finds*, WASH. POST, Jan. 25, 2019 available at https://www.washingtonpost.com/technology/2019/01/25/amazon-facial-identification-software-used-by-police-falls-short-tests-accuracy-bias-new-research-finds/?noredirect=on&utm_term=.3014ef154f26.

13. PATRICK J. GROTH ET AL., REPORT ON THE EVALUATION OF 2D STILL-IMAGE FACE RECOGNITION ALGORITHMS, NIST Interagency Report 7709

at 2, National Institute of Standards and Technology (Aug. 24, 2011), available at http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=905968 ("Face images have been collected in law enforcement for more than a century, but their value for automated identification remains secondary to fingerprints.").

14. P. JONATHON PHILLIPS ET AL., FACE RECOGNITION ACCURACY OF FORENSIC EXAMINERS, SUPERRECOGNIZERS, AND FACE RECOGNITION ALGORITHMS 1 (Proceedings in the National Academy of Sciences) (2018), available at <https://doi.org/10.1073/pnas.1721355115> (finding that "The best machine performed in the range of the best humans: professional facial examiners.").

15. CLAIRE GARVIE, GARBAGE IN, GARBAGE OUT: FACE RECOGNITION ON FLAWED DATA, GEORGETOWN PRIVACY CENTER AND THE LAW (2019), <https://www.flawedfacedata.com>.

16. See PATRICK J. GROTH ET AL., *supra* note 13 (explaining that facial recognition algorithms produce better results on visa images than on mugshots because the visa images are more standardized and have less variation in "pose, illumination and expression variation").

17. BRENDAN F. KLARE ET AL., FACE RECOGNITION PERFORMANCE: ROLE OF DEMOGRAPHIC INFORMATION, *Transactions on Information Forensics and Security* 1789 at 1 (2012) (finding that "Sources of errors in automated face recognition algorithms are generally attributed to the well-studied variations in pose, illumination, and expression, collectively known as PIE. Other factors such as image quality (e.g., resolution, compression, blur), time lapse (facial aging), and occlusion also contribute to face recognition errors.").

18. GARVIE ET AL., *supra* note 4 (explaining that "In the 'wild,' photos rarely contain the frontal images that face recognition algorithms prefer. Poor and uneven lighting can confuse algorithms that rely on facial features or skin textures. Algorithms have an especially tough time mixing photos taken in different circumstances, like mug shots and surveillance camera stills.").

19. CLAIRE GARVIE, GARBAGE IN, GARBAGE OUT: FACE RECOGNITION ON FLAWED DATA, GEORGETOWN PRIVACY CENTER AND THE LAW (2019), <https://www.flawedfacedata.com>.

20. CLAIRE GARVIE, GARBAGE IN, GARBAGE OUT: FACE RECOGNITION ON FLAWED DATA, GEORGETOWN PRIVACY CENTER AND THE LAW (2019), <https://www.flawedfacedata.com/> (referencing a case where "One detective from the Facial Identification Section (FIS), responsible for conducting face recognition searches for the NYPD, noted that the suspect looked like the actor Woody Harrelson.... A Google image search for the

FORENSIC DNA CONSULTANT

LISA MOKLEBY

B.Sc., M.S.F.S.

306-960-7495

- Trial preparation/ assistance
- DNA case file review and data interpretation
- Expert witness testimony
- Can educate and give lectures on DNA



AURORA FORENSICS

check out my website:

WWW.AURORAFORENSICS.CA

actor predictably returned high-quality images, which detectives then submitted to the face recognition algorithm in place of the suspect's photo.").

21. *Id.*

22. BRENDAN F. KLARE ET AL., *supra* note 17 (finding that "[T]he performances of three commercial face recognition algorithms were measured. The performances of all three commercial algorithms were consistent in that they all exhibited lower recognition accuracies on the following cohorts: females, blacks, and younger subjects (18 to 30 years old).").

23. JOY BUOLAMWINI & TIMNIT GEBRU, GENDER SHADES: INTERSECTIONAL ACCURACY DISPARITIES IN COMMERCIAL GENDER CLASSIFICATION (Proceedings of Machine Learning Research 81:1-15) (2018), available at <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>.

24. GARVIE ET AL., *supra* note 4 (expressing that "Age changes faces, as do cosmetics, inebriation, and obstructions like glasses or hair.").

25. Ben Austen, *What Caricatures Can Teach Us About Facial Recognition*, WIRED (2011), https://www.wired.com/2011/07/ff_caricature (noting that "To crack the problem of real-time recognition, however, computers would have to recognize faces as they actually appear on video: at varying

distances, in bad lighting, and in an ever-changing array of expressions and perspectives. Human eyes can easily compensate for these conditions, but our algorithms remain flummoxed.”).

26. See, e.g., Austen, *supra* note 2.

27. If mass surveillance with real time FRS ever becomes prevalent enough to track people’s movements over a period of time, then attorneys might also consider raising privacy challenges using the reasoning in *Carpenter v. United States*, 484 U.S. 19 (1987).

28. See *Haliym v. Mitchell*, 492 F.3d 680, 706 (6th Cir. 2007) (opining that “Witnesses are very likely to recognize under any circumstance the people in their lives with whom they are most familiar, and any prior acquaintance with another person substantially increases the likelihood of an accurate identification.”).

29. Lynch, *supra* note 1.

30. Joseph Goldstein, *Jailing the Wrong Man: Mug Shot Searches Persist in New York, Despite Serious Risks*, N.Y. TIMES (Jan. 5, 2019), available at <https://www.nytimes.com/2019/01/05/nyregion/nypd-mug-shots-false-identification.html> (discussing mugshot searches where persons are included in the procedure only because they have a mugshot in a database).

31. See, e.g., *Holt v. United States*, 218 U.S. 245, 252–53 (1910) (finding that “the prohibition of compelling a man in a criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material.”); *United States v. Wade*, 388 U.S. 218 (1967) (holding that “compelling the accused merely to exhibit his person for observation by a prosecution witness prior to trial involves no compulsion of the accused to give evidence having testimonial significance.”).

32. See *People v. Johnson*, 139 Cal. App. 4th 1135, 1150–51 (2006) (explaining in dicta that “Whether facial recognition software is discerning and accurate enough to select the perpetrator ... is immaterial: what matters is the subsequent confirmatory investigation.”).

33. *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579 (1993); *Frye v. United States*, 293 F.1013 (D.C. Cir. 1923).

34. *People v. Roland*, No. 3876-2016 (Qns. Cty. May 15, 2017).

35. *Id.*

36. Lynch, *supra* note 1.

37. OVERVIEW OF FACE DETECTION AND RECOGNITION, AMAZON RECOGNITION DEVELOPER GUIDE (2019), available at <https://docs.aws.amazon.com/rekognition/latest/dg/face-feature-differences.html> (explaining

that “Confidence scores are a critical component of face detection and recognition systems.”).

38. GARVIE ET AL., *supra* note 4.

39. Rebecca Wexler, *Life, Liberty and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1367 (noting that “Other areas where trade secrets may arise in defense challenges to investigative technologies include face recognition and predictive policing. Some police departments have denied open records requests for the user manuals for face recognition systems by citing trade secrets exemptions to their disclosure obligations.”).

40. *Id.* at 1397 (explaining that “New York City’s Office of the Chief Medical Examiner (OCME) has argued, repeatedly and successfully, that the source code for a forensic [DNA] software program developed in house using taxpayer funds should be protected from subpoena by criminal defendants.”).

41. Vera Eidelman, *Secret Algorithms Are Deciding Criminal Trials and We’re Not Even Allowed to Test Their Accuracy*, ACLU SPEECH, PRIVACY, AND TECHNOLOGY PROJECT, Sept. 15, 2017, available at <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/secret-algorithms-are-deciding-criminal-trials-and>.

42. *Brady v. Maryland*, 373 U.S. 83 (1963).

43. See, e.g., *Boyette v. Lefevre*, 246 F.3d 76, 91 (finding that documents were *Brady* material because they could have helped the defense suggest an alternative perpetrator); *United States v. Robinson*, 39 F.3d 1115 (10th Cir. 1994) (overturning a conviction where prosecution did not disclose that eyewitness said the perpetrator “may” have had characteristics tending to match the co-defendant).

44. See, e.g., *Lefevre, supra* note 43 (finding a witness statement about uncertainty of the identity of her attacker to be “classic *Brady* material.”); *Jacobs v. Singletary*, 952 F.2d 1282 (11th Cir. 1992) (finding a *Brady* violation when the state withheld a polygraph report about an eyewitness’s lack of certainty about what he saw); *Conley v. United States*, 332 F. Supp. 2d 302 (D. Mass. 2004), *aff’d*, 415 F.3d 183 (1st Cir. 2005) (finding a *Brady* violation when prosecution withheld memo stating that witness was uncertain of his recollection of events).

45. *Sellers v. Estelle*, 651 F.2d 1074, 1077 (5th Cir. 1981) (finding exculpatory evidence in the form of inadmissible hearsay to be *Brady* material).

46. See *Manson v. Brathwaite*, 432 U.S. 98 (1977).

47. See *Watkins v. Sowders*, 449 U.S. 341 (1981) (holding that there is no

constitutional mandate for courts to hold pretrial suppression hearings with regards to identifications, but noting that it is the better practice).

48. *Simmons v. United States*, 390 U.S. 377, 384 (1968).

49. *Styers v. Smith*, 659 F.2d 293, 297 (2d Cir. 1981) (finding that “notification to a witness that a suspect has been picked up will not automatically result in suppression of the witness’s subsequent identification testimony ... [however] this procedure may be dangerously suggestive when combined with a showup rather than a fair lineup.”).

50. *Brathwaite, supra* note 46 at 116 (explaining that “identifications arising from single-photograph displays may be viewed in general with suspicion. ...”).

51. Case assigned to the author. Case date not provided for reasons of client confidentiality.

52. See *Wade, supra* note 31.

53. See *Summitt v. Bordenkircher*, 608 F.2d 247, 250–51 (6th Cir. 1979), *aff’d sub nom. Watkins v. Sowders*, 449 U.S. 341 (1981) (“The purpose that a voluntariness hearing is designed to serve has nothing whatever to do with improving the reliability of jury verdicts. ... The basis of the due process right against suggestive identification procedures is significantly different. It is, first of all, apparent that the primary evil to be avoided is a very substantial likelihood of irreparable misidentification.”) (internal citations omitted).

54. See *Manson v. Brathwaite*, 432 U.S. 98 (1977) (holding that it was not error to admit a pretrial identification that was both suggestive and unnecessary because there was not a substantial likelihood of irreparable misidentification).

55. *State v. Moore*, 188 N.J. 182 (2006). ■

About the Author

Kaitlin Jackson is a Public Defender at Bronx Defenders. Previously, she worked at the National Registry of Exonerations and the Legal Aid Society of Nassau County in New York.



Kaitlin Jackson

Bronx Defenders
Bronx, NY
718-838-7820

EMAIL kaitlinj@bronxdefenders.org

WEBSITE www.bronxdefenders.org

TWITTER @BronxDefenders