Expert Witness Report by Dr. Michael C King

Robert Williams v. City of Detroit et al., No. 21-cv-10827 (E.D. Mich.)

May 26, 2023

Professional background and qualifications

1. I am a research scientist at the Florida Institute of Technology's (FIT) Harris Institute for Assured Information and have served in this role since August 2015. I also hold a joint appointment as an Associate Professor in the FIT College of Engineering and Sciences' Department of Computer Engineering and Sciences. (The department's name will change to the Department of Electrical Engineering and Computer Sciences on July 1, 2023.) I hold a Doctor of Philosophy degree in Electrical Engineering from North Carolina Agricultural and Technical State University (2001).
2. Prior to joining academia, I served 14 years (Aug. 2001 – Sept. 2015) as a scientific research/program management professional in the United States Intelligence Community.
3. While in government, I created, directed, and managed research portfolios covering various topics related to biometrics and identity, including advanced exploitation algorithm development, advanced sensors and acquisition systems, and computational imaging.
4. More specifically, many projects under my supervision were developed to enhance the intelligence community's ability to extract biometric features from low-quality image and video media. The goal was to provide tools that would enable intelligence analysts to answer the question of who is this person that appears in the image/video or if this person has been seen before.
5. A large emphasis of the research was focused on advanced capabilities related to face recognition in non-ideal data (e.g., surveillance video).

6. To that end, I crafted and led the Intelligence Advanced Research Projects Activity's (IARPA) Biometric Exploitation Science and Technology (BEST) Program, successfully transitioning technology deliverables to over 40 Government organizations.

7. The scope of work for the BEST Program focused on the study and development of techniques/methods to address the challenges of the science of biometric recognition—the level of confidence associated with a match/non-match of biometric signatures. The overarching goals for the IARPA BEST Program were: 1) to significantly advance the Intelligence Community's (IC) ability to achieve high-confidence match performance, even when the features are derived from non-ideal data; and 2) to significantly relax the constraints currently required to acquire high fidelity biometric signatures. The signatures researched in the program were limited to the **face**, iris, and speaker biometric modalities.

8. As a Subject Matter Expert in biometrics and identity intelligence, I was invited to brief the Director of National Intelligence (4x), Congressional staffers and science advisers, Defense Science Board, Army Science Board, and Intelligence Science Board on matters related to biometrics and identity intelligence.

9. I also served as Intelligence Community Department Lead to the White House Office of Science and Technology Policy's (OSTP) National Science and Technology Council Subcommittee (NSTC) on Biometrics and Identity Management (2005 – 2012).

10. Additionally, I worked for the National Security Agency as Technical Director (2002 – 2005) in the Research Directorate's Human Interface Security Research Focus Area. Most of the research conducted by this team focused on addressing key challenges related to detecting and extracting uniquely identifiable features from faces appearing in low-quality images and videos.

11. My final Government appointment was as Director of Applied Research and Innovation in the Directorate of Science and Technology's Office of Technical Services at the Central Intelligence Agency. In this role, I led a team of scientists in delivering advanced capabilities in cyber, identity intelligence, and special communication systems.

12. Since transitioning into academia, I have worked to develop a research program focused on the areas of personal identification. More specifically, research interests in the areas of biometrics (i.e., face and iris recognition) and uniquely identifiable signatures leaked into the cyber domain.

13. I also teach a course entitled "Biometric Authentication Technologies" as part of the master's degree program in Information Assurance and Cybersecurity. The course is available to master's and doctoral-level students in electrical and computer engineering and computer science concentrations. In addition to covering biometrics more broadly, the course provides a more comprehensive treatment of the face, iris (eye), and fingerprint modalities.

14. I have secured research awards of over $13 million in funding as principal investigator related to the protection and privacy of identities in cyber; computational psychology; long-range face recognition; and the study of demographic effects related to face recognition.

15. The project related to the demographic effects of face recognition was initiated due to widespread criticism of face recognition technologies used by law enforcement and media reporting of the technology not being as accurate on people with darker skin tones. The project started in the spring of 2018 in collaboration with a senior faculty member at the University of Notre Dame. This collaboration has resulted in approximately 15 articles

dealing with various aspects of demographic effects on face recognition accuracy since 2019. A list of my publications is contained in the curriculum vitae attached to this report.

16. I currently serve as a technical expert on the National Academy of Science, Engineering, and Medicine's committee on Facial Recognition: Current Capabilities, Future Prospects, and Governance. The US Government sponsors the study to assess current capabilities, future possibilities, and societal implications of facial recognition (FR) technology governance.

17. I have been retained in this case by counsel for Robert Williams as an expert on facial recognition technology. I am performing this service at a rate of $255 per hour.

Purpose and scope of this report

18. In this report, the primary objective is to provide an assessment related to the use of automated face recognition (AFR) technology, ultimately leading to the wrongful arrest of Mr. Robert Williams.

19. AFR technology is a tool used increasingly by law enforcement to attempt to identify a suspect whose face has been captured on surveillance video or in an image. The technology compares an image of the suspect's face, often called a probe image, to large repositories (often on the order of millions) of mugshots, driver's license photos, state IDs, etc., in search of a person with facial characteristics closely matching that of the suspect. The process does not yield—nor is it expected to—a positive identification. It returns a list of candidate images for persons that the algorithm determines have facial characteristics similar to the suspect being searched for.

20. To that end, my primary focus is on providing insights on the images used to conduct the search, the face recognition algorithms used, the size of the gallery, and the weight given to

an investigative lead resulting from a facial recognition search. Unless otherwise noted, my opinions herein are based on my expertise, training, and experience with development, use, testing, and evaluation of facial recognition technology, and reflect methodologies and techniques widely accepted within my field.

Background on case

21. The following is based on review of materials provided to me by counsel for Robert Williams in this litigation. On October 2, 2018, an unknown person was captured on video surveillance cameras stealing watches from a Shinola store in Detroit. The surveillance video was recorded and stored.

22. The Detroit Police Department ("DPD") was notified of the theft on October 6, 2018. An analyst from the security firm employed by Shinola provided five videos and three still images captured from frames of one of the videos to DPD.

23. The three still images were of low quality. The suspect's face in each image was partially occluded by a baseball cap, showed the presence of shadows, poorly lit, and captured from an angle, and it had a low pixel density. The person pictured in the image appeared to be African American.

24. A DPD detective provided the images to the DPD Crime Intelligence Unit ("CIU") and asked for a face recognition search to be conducted on the unknown suspect depicted in the images.

25. A CIU employee received the request for a face recognition search and the three still images. Although DPD had access to two face recognition systems from the company DataWorks Plus (one that it licensed under a contract with DataWorks Plus, and one it had access to through an agreement with the Michigan State Police), the CIU employee did not

run a facial recognition search themselves and instead forwarded the request for a face recognition search to the Michigan State Police ("MSP").

26. The request was submitted to MSP to run the face image through its system on March 8, 2019.

27. An MSP employee selected one of the three images to use in the facial recognition search. An image submitted for a facial recognition search is often known as a "probe image." She cropped the probe image to focus on the suspect (as opposed to the other individuals in the image) before conducting the facial recognition search.

28. The MSP employee conducted the facial recognition search using an internal system from DataWorks Plus and an external FBI system.

29. The internal DataWorks Plus system used two face recognition match engines (Rank One Computing ("ROC") and NEC Corporation) in its analysis. The database being searched for potential matches contained approximately 49 million images, including current and expired Michigan driver's license and state ID photos, arrest photos from law enforcement agencies across the state, and certain photos from the state Department of Corrections. Both engines search that same database; but each uses its own proprietary algorithm when searching the database, meaning that the two search engines typically will not yield completely overlapping results.

30. The ROC and NEC face recognition match engine in the DataWorks Plus system each returned 243 potential candidates (i.e., possible matches to the probe image) for further analysis. In depositions in this case, MSP personnel testified that when they run a search, each of these match engines returns either 243 candidate matches or zero candidate

matches. In this case, both match engines returned 243 results, in total there were 486 images of people returned in the candidate list as potential matches.

31. The FBI system, which either returns 50 candidate matches or 0, did not return any potential matches or candidates in this search.

32. A driver's license photo of Mr. Williams surfaced in the ninth position in the 243-person candidate list from the search using DataWorks Plus's ROC match algorithm. The license photo was from an expired license, not Mr. Williams's then-current license. The then-current license photo was also in the matching database, but did not return as a candidate match. DataWorks's NEC match algorithm did not include any of Mr. Williams's license photos in its 243-person candidate list.

33. The MSP image analyst, from visual inspection, selected the photo of Mr. Williams as a potential match and performed a morphological face comparison.

34. The image analyst reported that they were able to identify several features that were consistent between the probe image and the image of Mr. Williams. However, the image analyst also recorded the quality of the probe image as "poor" and recorded that the "overall head shape," overall face shape," "hairline," "ears," "forehead/brow ridge," "eyebrows," "chin/jawline," and "neck" were obstructed or not visible.

35. The probe image and the license photo of Mr. Williams were forwarded to an MSP supervisor to be validated on March 11, 2019 at 12:00 pm. Four minutes later, at 12:04 pm, the supervisor approved the analyst's determination.

36. The analyst then forwarded the match as an investigative lead to DPD on March 11, 2019. An employee in DPD CIU received the investigative lead from MSP and forwarded it to the lead DPD detective. No CIU personnel attempted to conduct an independent

comparison or evaluation of whether the probe photo of the unknown suspect and the investigative lead photo of Mr. Williams appeared to depict the same person.

37. On July 30, 2019, DPD included a photo of Mr. Williams in a 6-pack photo array and showed it to the representative of Shinola's security contractor to compare. The security company representative, who had never seen the suspect in person and had only watched the same security footage that was in DPD's possession, compared the photo of Mr. Williams to images from selected surveillance video frames and identified Mr. Williams as a match to the suspect.

38. A warrant request was made on August 25, 2019. On August 28, 2019, the warrant was entered into the Michigan Law Enforcement Information Network (LEIN).

39. On January 9, 2020, members of the Detroit Police Department visited Mr. William's home to arrest him for the Shinola theft.

40. On January 10, 2020 Mr. Williams was released on a personal bond.

41. On January 13, 2020, the detective working the case determined that Mr. Williams was not the person observed in the video. Charges against Mr. Williams were subsequently dropped.

Materials that were reviewed

42. Video from Shinola store.

43. Images (i.e., frames) taken from Shinola video and cropped probe image used by MSP for facial recognition search.

44. Email correspondence between DPD and MSP and within MSP concerning the facial recognition search request and results; MSP investigative lead report; MSP investigative lead report supplemental information sheet; DataWorks Plus solicitation response to DPD; MSP

documentation concerning Statewide Network of Agency Photos (SNAP) and facial recognition searches; request for warrant and associated documents prepared and submitted by Detective Bussa.

45. Transcripts of depositions of Krystal Howard, Jennifer Coulson, Levan Adams, Benjamin Atkinson, Donald Bussa, Rathe Yager, Deputy Chief Franklin Hayes, Nathan Howell, and John Fennessey.

Background on automated facial recognition technology

A. What is automated facial recognition technology?

46. AFR is a form of biometrics technology used to 1) verify a claimed identity (i.e., 1:1—verification mode) or 2) determine the identity of an unknown person by searching a large repository (i.e., 1:N—identification mode). 1:1 verification is used to confirm someone's identity, for example, when a mobile phone takes an image of your face and compares it to a single image of the owner to determine if you are the owner of the phone. 1:N searches, which are the focus of most of this report, are the type typically used by law enforcement agencies (and other users) to attempt to identify an unknown person believed to be involved in a crime or otherwise of interest. To accomplish either task, face recognition employs a computer algorithm to analyze faces appearing in two distinct photographs and produces a score measuring the degree of similarity between the two faces. I will refer to this as a "similarity score." (Note: In depositions that I have reviewed, it is also sometimes referred to as a likelihood score or confidence score.)

47. Facial recognition algorithms are not designed to determine with certainty that two photos are or are not a match. Thus, the similarity score is not discreet in that it is either a 1 ("match") or 0 ("no match") but can take on a range of values. Nor is a score directly tied

to some statistical degree of confidence in the classical sense. In general, the higher the score, the more similar the faces, but results appearing in the candidate list with the highest scores may not be a true match to the probe photo. (Note: alternatively, scores may also be computed as a distance measure, meaning the lower the score, the more similar. But most systems in use today use some form of similarity measure. Therefore, I will use the term "similarity score" throughout this document.)

48. AFR systems typically implement a criterion based on the similarity score meeting or exceeding a threshold to determine whether a match has been made. In 1:N (identification) searches, the system will typically return a number of results consisting of potential candidate matches, beginning with the image with the highest similarity score determined by the system. The system can be set, as MSP's appears to be, to return a fixed number of results, regardless of their similarity scores, or to only return results that exceed a certain similarity score, in which case the number of results returned will vary from search to search.

49. The process of face recognition typically follows the following steps.

    a) Input an image (known as the probe image).

    b) Detect and isolate the region of pixels representing the face. (Note: An algorithm may sometimes fail at this stage if it cannot detect a face. This failure may be reported by the system as a *"failure to detect" or "failure to acquire."* The operator may manually select the image region containing the face if the system has a user interface and allows human assistance.)

    c) Apply preprocessing routines—this often involves the facial recognition engine automatically resizing the image without user input to match the size required to extract facial features and applying enhancement techniques to improve the quality of the image.

d) Extract facial features, called a template, to capture unique aspects of the person's face. (An algorithm may sometimes fail at this stage if the image is degraded to the point that reliable features cannot be extracted. This failure may be reported by the system as a *"failure to generate a template" or "failure to enroll."* This type of failure would require more extreme image enhancements for further processing, if the probe image could be used at all.) A template is, in essence, a mathematical description of the features of the face pictured in the image.

e) Compare the person's template to 1 or more templates stored in a gallery (typically a database of photos), in search of a match. A gallery could be large (e.g., millions of photos in a state driver's license database such as MSP's) or small (e.g., photos of individuals recently arrested on a particular charge). Each photo in a gallery is associated with its own template. This process is known as "feature matching."

f) Compute a similarity score for comparisons made to each image in the gallery. To facilitate the rapid search through a large repository of images, all steps in the process necessary to generate a face template for images in the gallery are performed in advance, with the templates being stored in a database (i.e., gallery). This is one place where the difference between various algorithms is important, as described below, since each algorithm will have its own mathematical way of representing and comparing the similarity of the probe image's template to the templates in the gallery.

g) Depending on the system's configuration, the similarity score for each image comparison may then be assessed relative to a pre-determined threshold to determine if a match has been made. A similarity threshold (also sometimes known as a likelihood threshold or confidence threshold) is a cutoff below which the system will not show candidate matches. For example, if a system is programed with a similarity threshold of .980, then only candidate matches with similarity scores of .980 or above will return as results visible to the AFR operator. Alternately, systems may be configured without a threshold, meaning the system will return candidate match results regardless of how high or low their similarity score is.

50. The process described above is illustrated in Figure 1 This illustrates person "A" (Caucasian female—top) being compared to person "B" (African American Male—bottom) using a single face recognition algorithm. The face detection and preprocessing steps could vary for the two images. However, images for each person must go through the same feature extraction process as it is unique to each face recognition algorithm and designed in concert with the feature matcher. In this example, the two people are clearly not the same. Thus, it is desired for the recognition system to produce a low score indicating a non-match.

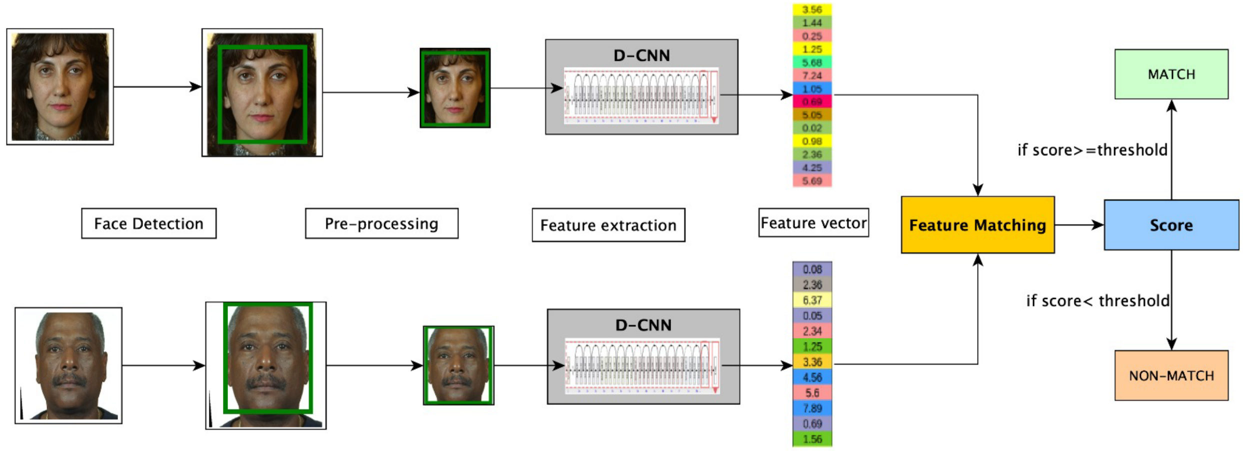

Figure 1: Typical face match process (For illustration purposes only.)

51. It is important to note that different developers of face recognition algorithms will use various mathematical models in their respective algorithms to produce a similarity measure. There is not a single set of mathematical formulations used by every vendor. And changes are constantly being made to the algorithms themselves in hopes of improving speed, accuracy, and efficient use of a computer's available memory.

52. There is no universal "score" which constitutes a "match" that applies to every algorithm. And the range for the maximum and minimum scores an algorithm produces can vary widely. Therefore, each algorithm must be measured on its own merit to determine the degree of confidence that may be placed on a score generated in any given circumstance.

53. Each vendor typically recommends the optimal similarity threshold setting for the face recognition algorithm relative to the customer's accuracy requirements. This setting serves to moderate two types of errors that can be made by the system. A false positive identification error occurs when the system reports a score high enough for the system to report a match when comparing two images that are not of the same person (i.e., a non-mated comparison). This leads to a false identification. The second type of match error, a

false negative identification, is when the system reports a score that is too low to be considered for a match when comparing two images of the same person (i.e., mated comparison). This leads to the system reporting no match when in fact there is an image in the gallery of the person shown in the probe image.

54. The process described in Figure 1 is intended to illustrate for generating a match score for two images. In an operational scenario, templates will have already be generated for every image in a repository (i.e., database). Therefore, when a comparison is to be made, the system only needs to complete the entire process of generating a template for the new probe image. Once the template for the probe is generated, it can be quickly and automatically compared to 1 or all of the templates representing images in the gallery in search of a match without any further human intervention.

B. What do independent evaluations say about automated face recognition accuracy?

55. Through its Face Recognition Vendor Test Program (FRVT), the National Institute for Standards and Technology (NIST) has been reporting on advances in the accuracy of face recognition algorithms for over two decades. Recent studies in the NIST FRVT1:N identification track show dramatic improvements in the last 7-10 years, with reported accuracy rates as high as 99.99% for top performing algorithms under ideal conditions on a database of 12 million mugshots images [1].

56. There are two observations also shared in NIST FRVT reporting with relevance to this case.

a) First, while the NIST FRVT reports are quite comprehensive, it's impossible to capture and assess accuracy under the full slate of conditions encountered in uncontrolled operational settings. And to NIST's credit, they allude to this fact by including the following language in their report: "Given algorithm-specific variation, it is incumbent upon the system owner to know their algorithm. While publicly available test data from NIST and elsewhere can inform owners, it will usually be informative to specifically measure accuracy of the operational algorithm on the operational image data, perhaps employing a biometrics testing laboratory to assist." [2].

b) Secondly, and perhaps most relevant to this case, some systems are specifically configured to return a set number of images (i.e., candidates) with every search. The report also states that "In such cases, the false positive identification rate is 100% because any search of someone not in the database will still yield candidates" [2].

57. The gains in accuracy are mainly attributed to the introduction of deep convolution neural networks (DCNN) as the computation engine for learning features for pattern recognition to the field of face recognition [3]. DCNNs are highly complex mathematical models that learn what facial features are important for matching images of a person. These complex models are not readily interpretable by humans, making it impossible to tell which facial features the models have deemed important for matching images. There are many aspects of the DCNN training process that are highly proprietary, and details are not publicly available.

58. However, accuracy rates can vary widely between different facial recognition algorithms, with some algorithms performing with markedly less accuracy than others. Additionally, the accuracy of a facial recognition algorithm's results depends heavily on factors including the quality of the probe image and the demographics (including skin tone) of the

person depicted. As discussed below, searches such as comparisons of passport photos, which all feature nearly uniform proportions, facial expressions, and poses, are most accurate; searches using lower quality probe images can generate significantly less accurate results.

59. The reason image quality matters is that lower-quality probe images contain less interpretable facial data for the algorithm to process and analyze. As described above, AFR algorithms must extract facial features from an image in order to create a mathematical template that can be used for automated comparisons. Factors such as partial obstruction or occlusion of the face, low lighting, over- or under-exposure of the image, face angled away from the camera, shadows on the face, and low pixel count all reduce the number or clarity of facial features, thus degrading the system's ability to produce a template of sufficient quality to produce a reliable comparison to templates in the stored gallery of comparison images.

C. Longstanding concerns regarding automatic face recognition and use of by law enforcement

60. Even as NIST has continued to track advancements being made by AFR technology, researchers, policy makers, and privacy advocates have warned of the potential harmful effects of its use by law enforcement.

61. In 2016, the Georgetown Law Center for Privacy and Technology released a report entitled The Perpetual Lineup [4], sounding the alarm on how face recognition may be used by law enforcement to search large state image repositories for persons suspected of committing a crime. Additionally, the report brought attention to how the technology may "disproportionately affect African-Americans" and warned of the technology having the potential to be least accurate on this group.

62. Buolamwini and Gebru [5] published the results of their study called “Gender Shades” which applied technologies derived from the face recognition domain to classify a person’s gender. The study reported that the gender classifiers they studied were most accurate for light-skinned males, and markedly less accurate for dark-skinned females.

63. Concerns over the use of face recognition technology have even made it to Capitol Hill. On March 22, 2017, there was a congressional hearing on “Law Enforcement’s Use of Facial Recognition Technology” [6]. Senior officials representing the Homeland Security and Justice Departments, U.S. Government Accountability Office, NIST, Federal Bureau of Investigation, NEC Corporation of America, and the Electronic Frontier Foundation were called to give testimony, with some testimony expressing significant concern about demographic disparities in accuracy [7].

64. The controversy over the use of face recognition technology also led to numerous articles being published. Articles highlighting the lack of accuracy of the technology even caught the attention of reputable news outlets such as the *New York Times*, which published an article entitled “Facial Recognition Is Accurate, if You're a White Guy” in February of 2018 [8].

65. More recently, a study has found the use of face recognition technologies contributes a greater disparity in arrests [9]. The authors report “statistically meaningful and positive FRT effects on Black arrest rates and negative effects on White rates.”

D. Discussion of face recognition differential inaccuracy relative to different demographics

66. Given the growing concerns related to face recognition technology being used by law enforcement and reports that it was inaccurate on African Americans and women, I initiated a study in close collaboration with Dr. Kevin Bowyer, Schubmehl-Prein Family

Professor in the Department of Computer Science and Engineering at the University of Notre Dame. The research project began in June 2018 with the objective of characterizing the accuracy of face recognition systems relative to demographic groups.

67. In addition to our team, a global community of scholars has been actively engaged in scholarly research to understand the role of demographics in the accuracy face recognition systems. This complements researchers in various components of the US Government such as NIST and the Department of Homeland Security.

68. In April of 2019, Dr. Bowyer and I released our first report (co-authored with our students), which found that the technology routinely gave higher scores for both non-mated and mated comparisons of the African-American demographic cohort than were produced for the their Caucasian counterparts [10]. The net effect of the non-mated comparisons giving higher scores for the African American cohort was an elevated false positive rate for that demographic cohort.

69. Findings reported by NIST in their FRVT report on demographics [2] published in December of 2019 were congruent with our research finding published in [10]. The NIST study employed a litany of algorithms and a much larger dataset that contained roughly 12 million images to report that "*false positive rates often vary by factors of 10 to beyond 100 times*" [2].

70. We conducted subsequent studies related to the subject that confirmed a correlation between darker skin tones and higher false positive rates. We have been unable to conclusively demonstrate the reason for this disparity (i.e., unable to conclude that the disparities in accuracy are *caused solely by* the darker skin tones), but we certainly conclude and lament that skin tone plays a role [11].

Use of automated facial recognition technology in this case

A. **Images of suspect extracted from store surveillance video recording**

71. The suspect, whose appearance is consistent with that of an African American male, was captured on surveillance video picking up five watches and placing them in his jacket/coat pocket.

72. The resolution of the video recording is 1920 (width) x 1080 (height) pixels.

73. An image analysis request for face recognition from a photo was submitted to the MSP by DPD Crime Analyst Rathe Yager of the DPD's Crime Intelligence Unit on March 8th, 2019. The request included 3 frames taken from the video. Each frame appears in its original format with a 1920 (w) x 1080 (h) pixels resolution. Several conflicting explanations have been offered as to why DPD submitted the request to MSP instead of running an analysis itself, though I am informed by Mr. Williams' attorneys that DPD officials have testified that they sometimes send facial recognition requests to MSP when DPD fails to identify a match itself, or because MSP has access to a larger image database to search against.

B. Search for suspect in the SNAP database using DataWorks Plus

74. MSP digital image examiner Jennifer Coulson conducted a facial recognition search of images in the Statewide Network of Agency Photos ("SNAP") using the DataWorks Plus system.

75. SNAP is a large repository of images of people in the state of Michigan. The images are in the form of Michigan state identification photos (including current and expired driver's

licenses), mugshots, and Department of Corrections photos, all of which are taken in controlled environments and considered to be high-quality.

76. In 2019, it was recorded that the repository contained approximately 49 million images. (The repository now contains approximately 55 million images.)

77. The SNAP repository was searched using a facial recognition system developed by DataWorks Plus. The system employs two face recognition match engines (i.e., algorithms): A face match algorithm developed by ROC circa 2018, and one developed by NEC circa 2011.

C. A low-quality probe image is generated and used in automated face recognition

78. As explained in her deposition, the MSP image analyst, Jennifer Coulson, selected one of the three frames for processing in the face recognition system. Coulson then cropped the image to isolate the suspect and eliminate other persons visible in the original full frame. The resolution of the cropped image was 297 (w) x 365 (h) pixels. The suspect's body (from the head to the knee) was visible in the photo. The cropped photo is shown below as Figure 2.

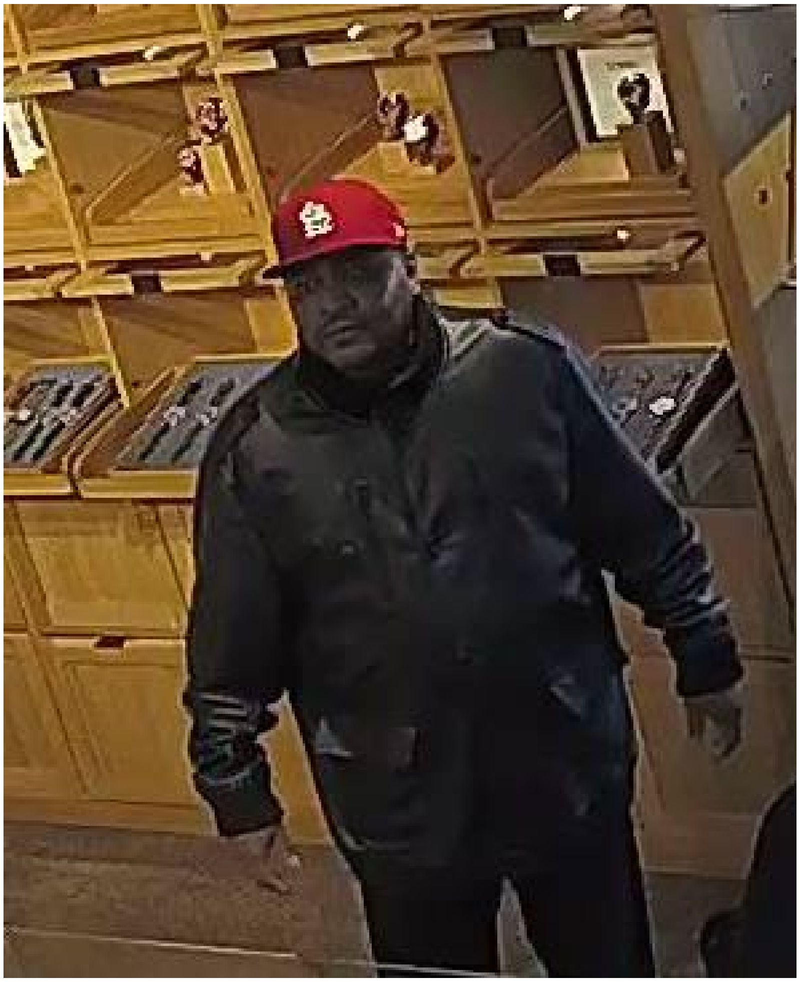

Figure 2: Probe photo produced by MSP image analyst.

79. This photo was ingested into the DataWorks Plus system. Ms. Coulson testified that she made no other alterations to the photo before conducting a search. It is unclear what, if any, image enhancement techniques may or may not have been applied automatically by the face recognition system.

80. In order for the system to run a search, the suspect's face would have to be isolated for processing as only the features extracted from the face itself can be used for the purposes of recognition. All other information contained in the images is useless and is eliminated.

81. The process of detecting and isolating the face in some cases may be performed by the analyst cropping the image only to show the face region. Here, however, because Ms.

Coulson testified to only cropping the image to produce Figure 2, the algorithm would have attempted to automatically detect the face for processing by the recognition system. Due to the reduced resolution of the image and without access to the algorithm used at the time of the search, I am uncertain as to whether this step could have been performed automatically by the algorithm without any assistance from the analyst. When the algorithm fails to detect the face, some systems will allow the analyst to draw a box around the subject of interest face or provide a tool to allow the analyst to pinpoint the location of the salient point on the face (e.g., eyes, nose, mouth, etc.) on the computer display.

82. I used the Microsoft Windows 11 Photos App to manually rotate the image clockwise by 13.2 degrees to estimate the image resolution used for processing. The rotation was performed to align the eyes on the zero-degree plane and minimize the occlusions on the face introduced by the hat the subject wore. The rotated image is shown in Figure 3.

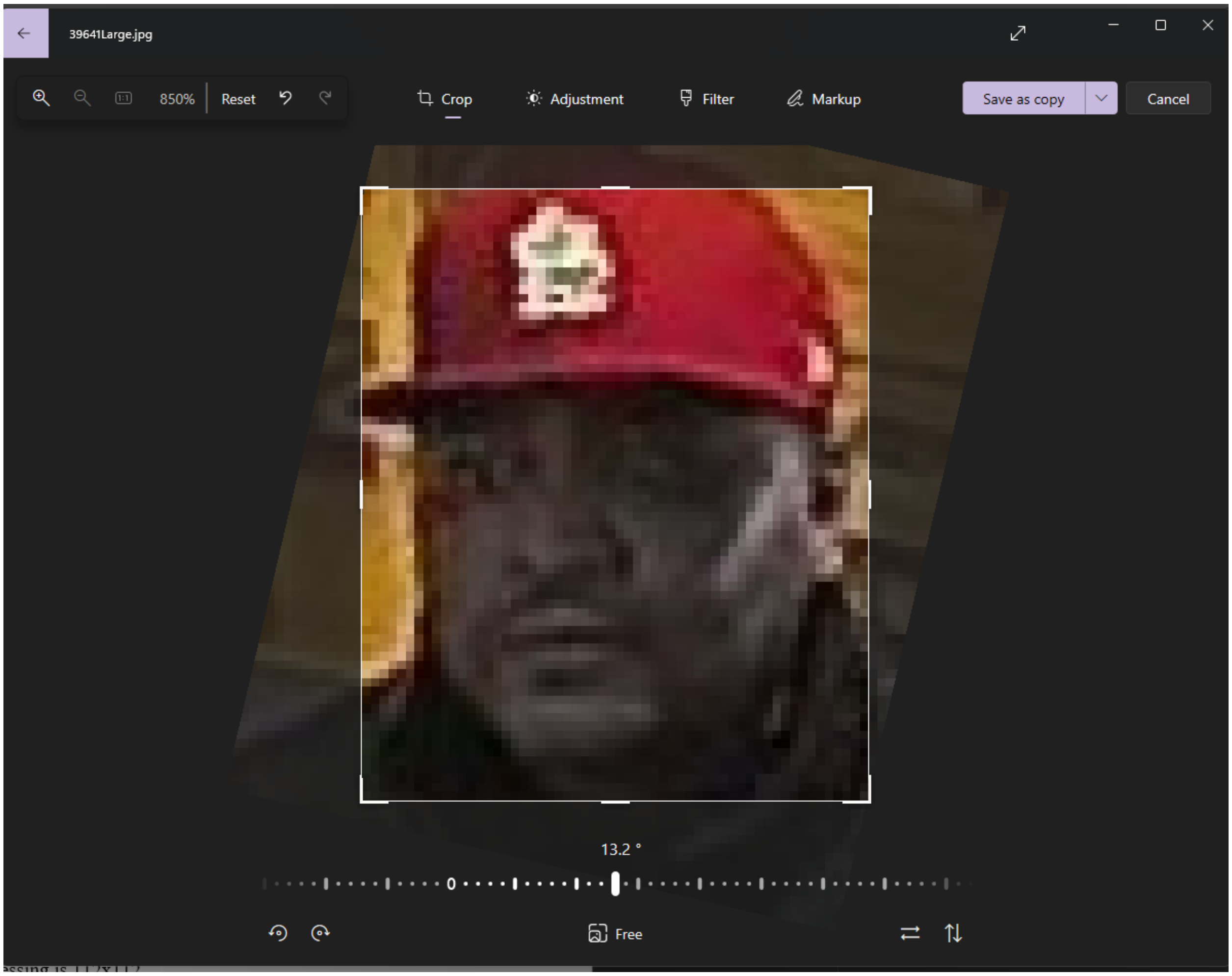

Figure 3: Rotated probe image with head region selected.

75. After rotating the image, I cropped the image to isolate only the face. The resulting probe image of the suspect’s face is estimated to have a 43 x 44 pixel resolution. The image is estimated to have an interocular distance (IOD) of approximately 17-20 pixels. The IOD is measured from the center point of one eye to the center point of the other eye. The cropped image of only the face is shown as Figure 4. (Note: These figures are not to scale and are included to provide visual context.)

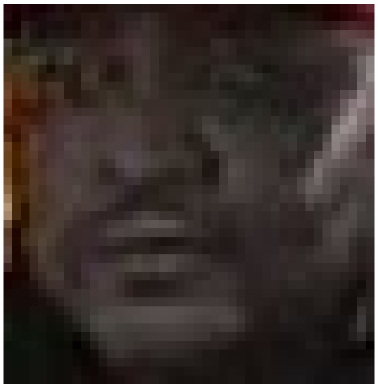

Figure 4: An illustration of what the final probe image may have looked like.

83. In Ms. Coulson's testimony, there is no indication that she assisted the DataWorks Plus algorithm to pinpoint the edges of the face in this manner. Figure 4 represents one possible result from detecting and isolating the face. However, given the reduced resolution of the image, the automated face detection may have produced a less precise cropping of the face. Surely the algorithm's representation would not yield the exact same result as the illustration in Figure 4. How, and the degree to which the differences would manifest themselves, is unknown.

84. The IOD is a widely accepted measure of image resolution used to evaluate the suitability of face images for processing by facial recognition search engines.

85. The NIST 2019 FRVT report on verification reported performance on datasets with corresponding IOD [8]. The datasets with corresponding IOD are as follows:

    a) Child Exploitation dataset images has a mean IOD of 70 pixels;

    b) visa images, 69 pixels;

    c) visa II images 61 pixels;

    d) mugshot images 113 pixels; and

e) webcam pictures, 38 pixels.

86. I am not aware of a large-scale evaluation being conducted with images that have a mean IOD of 17-20 pixels.

87. As the resolution (i.e., pixel count) of the image decreases, the system becomes less able to accurately assess the similarity of the probe image to images in the gallery. This is because as resolution decreases, the mated scores will get lower and begin to get approach the non-mated scores. The resulting effect is that the accuracy of the AFR system will also get lower.

88. Also evident from the image is spatially varying lighting and shadows on the suspect's face. Lighting also plays a significant role in the accuracy of a face recognition system. In prior work, Dr. Bowyer and I examined the influence of skin brightness on recognition similarity scores. We found that comparing image pairs with substantially different face brightness levels results in lower similarity scores. It is important to note that I did not have access to the native-format version of the driver's license photo or to the full SNAP database. But I find it reasonable to conclude that it would have been of higher quality from the perspective of illumination, and thus that the probe image and gallery photos would have had different face brightness levels [12].

89. The low resolution (as reflected by the low interocular pixel count) coupled with the shadows and low lighting on the subject's face, certainly played a signification role in the image analyst's assessment of the quality of the image as a probe as *"poor."*

90. The hat obscuring the subject's forehead, hairline, and top of head also reduced the image quality, by eliminating features that a facial recognition engine would normally rely on to attempt to produce candidate matches.

91. The individual factors (e.g., blur, resolution, pose, etc.) that adversely affect face recognition accuracy when measured independently are often interacting. The individual factors when combined have an even more pronounced effect resulting in reduced accuracy.

92. Given the image characteristics of the probe and its rating being poor, this certainly should have raised red flags both within the MSP and within the CIU of the DPD. Both organizations should have known via training or operational experience of the reduced likelihood of a legitimate face match being made from an image with these features. If they did not, then their training and experience had failed to acquaint them with even basic operation of the system, as this should have been obvious to any repeat user of facial recognition technology.

93. In my expert opinion, given the low quality of the probe image, DPD personnel who received the investigative lead report from MSP should have skeptical of the result when asking another agency to conduct a facial recognition analysis on the image. And they should have known and reiterated to DPD detectives that they should not rely on any resulting "lead" as a reliable match. (In fairness, it is printed in bold letters at the top of the investigative lead report, but the subsequent conduct of DPD detectives indicates that they either ignored or did not understand that printed warning.)

94. Also in my expert opinion, a quality gate should be used to filter out images that are not ideal based on objective measures (e.g., resolution, IOD, and brightness/contrast) that will be ingested into any AFR system used for processing. Doing so will eliminate many incorrect matches being promoted to the candidate list. While tailored to a particular vendor's match algorithm, a quality measure is usually a standard capability for

commercial AFR systems. The exact quality thresholds are adjustable and, in some cases, may be disabled (i.e., set to zero). Disabling the quality assessment filter essentially permits the algorithm to attempt to produce a comparable template for recognition regardless of the image's suitability.

D. Generating templates from the probe image for automated face recognition

95. As previously stated, the MSP's DataWorks Plus system integrated two face recognition match engines (i.e. ROC and NEC).

96. Besides the two algorithms directly integrated locally into MSP's DataWorks Plus system, it also provides an interface to a remote face recognition system operated and maintained by the Federal Bureau of Investigations (FBI). This allows for the probe image to be compared to the repository of face images maintained by the FBI.

97. Each algorithm will need to extract features from the probe image similar to the image shown in Figure 4 to construct a face template for comparison. The template size and feature extraction process are unique to each algorithm.

98. Given the timeframe of the development of the ROC algorithm, it is highly likely that the algorithm implements some form of a DCNN architecture. The exact construct of the architecture is proprietary. But one important factor is the size (i.e., pixel count) of the input to the DCNN feature extractor. The same is true for the AFR algorithm used in the FBI's system.

99. Most top-performing DCNN models that are freely available to the research community accept an image with dimensions 112x112 pixels. So the pixels on the face from a good-quality image would be down-sampled to match the dimensions of this resolution for input into the DCNN-based model (i.e., pixels are removed from the image to reach the desired

resolution while preserving salient features of the face). When this occurs, one can usually expect reliable performance from an AFR system.

100. Discussions I have had with leading vendors in the field while attending trade shows suggest some vendors have had success with reliably processing face images with 35 pixels between the eyes—with all other factors being nearly optimal (i.e., good illumination, limited occlusions, frontal pose, etc.). But they also suggest that by processing images with a resolution lower than 35 pixels between the eyes, the chances of a false match occurring is significantly increased.

101. That some commercial algorithms can process images of approximately 35 pixels between the eyes suggests that the input for their DCNN models are designed to process low-resolution surveillance-style images and likely accept an image as input slightly smaller than those used by open-source algorithms. I estimate the input resolution for a face image of approximately [70-90] x [70-90] pixels for commercial DCNN feature extraction model. Again, the exact dimensions are unknown. This information is also based on currently available technology. In 2019, the likely viable input size for doing an effective facial recognition search would have almost certainly been larger given the rapid rate of technological evolution in the field.

102. The dimensions for the image used in this case are approximately 43 x 44 pixels, which is significantly lower than what is estimated to be the input resolution of commercial algorithm design. When the image resolution is lower than the dimensions used in the design of the DCNN, the image's resolution must be increased (i.e., enhanced) through interpolation.

103. This interpolation process attempts to estimate information to fill in gaps for the new pixels that must be added. The more pixels added, the more information must be created. The added pixels do not, of course, provide an exact representation corresponding to those specific points on the face of the person in the probe image; rather, they are the algorithm's best estimate as to what features are consistent with the neighboring pixels. There are multiple techniques to facilitate this, but the exact implementation of the algorithm developer is not publicly available.

104. As the resolution of the probe image is reduced relative to that of the input to the DCNN model, the mated similarity scores will decrease and get closer to the high similarity tail of the non-mated score distribution; in other words, similarity scores for true matches and false matches will get closer. The role interpolation plays in this phenomenon is unclear. However, with this shift, it becomes unlikely that the AFR system will produce a similarity score high enough to be deemed a positive identification.

105. The architecture of the NEC AFR system is unknown. Given the date this system was reported to have entered into service, the NEC system is unlikely to implement a DCNN-based AFR engine. Therefore, it is unlikely that such a system would be capable of processing the poor-quality probe image generated for this case with any degree of accuracy.

E. Automated face recognition is used to search large repositories to identify suspect

106. The DataWorks Plus system searched against the approximately 49 million images in the SNAP repository accessible to Michigan State Police. The probe photo was also submitted to the FBI's system for comparison against the images in its repository; the number of images that were in the FBI's matching gallery is unknown.

107. Each face match engine (i.e., ROC and NEC) integrated into the DataWorks Plus system reportedly was configured to return 243 candidate images for further analysis as investigative leads. Since some people have multiple photos in the SNAP repository, it is impossible to arrive at the total number of unique persons represented in the candidate lists. From the depositions and the DataWorks proposal, it appears that the images in the candidate list are rank-ordered from high to low relative to the similarity score for each comparison.

108. According to the MSP image analyst, the FBI system returns exactly 50 candidates or 0 candidates for morphological processing by an analyst. In this search, the FBI system returned "zero" candidates as potential matches to the probe image ingested.

109. The reason for the FBI system not returning any candidates is unknown. However, it is well within reason to conclude that the FBI's system did not return any matches in this instance due to the probe image being of poor quality and, therefore, unable to extract reliable features for matching.

110. Being that there was no evidence of a technical error/issue (e.g., the network being down, FBI server not available, etc.), and the low quality of the probe image, this should have prompted additional scrutiny being placed on images being returned by the algorithms integrated into the DataWorks Plus system.

111. Another important factor pertaining to this search is the fact that as the number of subjects in the gallery and number of images per subject increases, the similarity scores for non-mated comparisons will also increase. In other words, as the size of the gallery increases, the incidence of false matches increases. This is because the likelihood of encountering people with similar facial characteristics (i.e., lookalikes, A.K.A. doppelgangers) as the

person being searched also increases. This phenomenon is reported by NIST [13] in a study conducted using a repository of high-quality images of 12 million subjects. The search conducted by MSP consisted of approximately 4x the number of images, with a poor quality probe photo, which further exacerbates the issue.

F. Examining the candidate lists

112. The candidate lists were populated with images that produced the highest similarity scores when compared to the probe image by each face recognition algorithm. It is worth noting that merely appearing in a candidate list does not mean the scores were high enough to qualify as a potential match by any credible statistical measure. It only means that they were the highest when compared to all other scores generated.

113. This is because the MSP system appears to be configured for what is commonly referred to as *lead generation*. In this configuration, the requirement that an image comparison meets or exceeds a threshold to be promoted to the candidate list is either disabled or the threshold is set sufficiently low to allow the candidate lists to be fully populated with each search of a probe image. In effect, the face system is tasked with searching through the large repository of images to identify a short list of potential matches. This large-scale search through 49 million images would be an intractable task for a human. In this case, the human's role is reduced to adjudicating which, if any, of the 486 candidates looks most similar to the person pictured in the probe image.

114. Given the disparity in age between the two algorithms, the size of the gallery searched, and the poor quality of the probe image, it is no surprise that images appearing in the candidate list produced by ROC did not appear in the candidate list produced by NEC. The actual number of common occurrences between the two lists is unknown.

115. Upon examining the ROC candidate list, the MSP image analyst determined that the image of Mr. Williams was the most viable candidate to perform a detailed morphological analysis on. The image of Mr. Williams in the candidate list was in the ninth position. The image analyst did not report results of a formal morphological analysis on any of the other 485 pictures that were returned in the two galleries that gave results.

116. It is reported that there were at least two images of Mr. Williams in the SNAP database. Based on a Michigan-issued driver's license expiring every four years [14]and the date of issue for Mr. Williams's current driver's license being 2021, the date of issue for the two driver's licenses in the SNAP database at the time of the AFR search is estimated as 2017 and 2013, although the dates the photos were taken could be earlier. (Note: No information provided to validate the actual date of issue.)

117. Only the older of the two images of Mr. Williams in the SNAP database produced a similarity score sufficient to be promoted into the ROC candidate list. The most current image—relative to the timeframe of the search—of Mr. Williams in the SNAP database did not appear in candidate lists produced by either AFR algorithm.

118. Since both driver's license photos would have been taken in a controlled setting and of high quality relative to the probe, the expectation would have been that the most current driver's license would have also surfaced in the candidate list. The absence of Mr. Williams's current driver's license photo in either algorithm's gallery should have been an obvious indicator that the "match" to his old driver's license was questionable. Any analytical explanation as to why this may have occurred is absent from the material provided.

119. Since each algorithm returns a candidate list of 243 subjects, even when a search *does* include a correct match within the results there could be as many as 242 people listed in

error (provided that no single person has multiple images returned in the candidate list.) This equates to roughly 99.6% error rate for people being presented to an image analyst as part of the candidate list—as a best case. When a face recognition system is configured to generate leads (i.e., when there is no similarity threshold set), the false positive rate is guaranteed 100% if the person being searched for is not in the gallery. And in this case, there was no guarantee that the suspect appearing the person appearing in the video from the Shinola store where the probe photo originated is in the SNAP repository being searched.

G. Human assessment of the candidate list

120. The MSP image analyst, from visual inspection, selected the photo of Mr. Williams, who was in the 9th position in the ROC results, as a potential match and performed a morphological face comparison.

121. The similarity scores produced by the algorithm for the comparisons of the probe image to images of Mr. Williams contained in the SNAP repository were not provided. Given that only the older photo of Mr. Williams surfaced in the candidate list, in the 9th position, while being compared to a poor quality probe image, I suspect the AFR generated score would have been well within the range of a false positive. Without the actual images to conduct an analysis, I cannot offer a definitive assessment.

122. And while the similarity scores are present in the DataWorks interface, the testimony provided by Coulson revealed that they are not used by the image analyst when completing the morphological comparison.

123. The supplemental lead report [BID-39641-19 SUPP.pdf] also lists 13 facial features corresponding to different parts of a person’s head and neck region.

124. There are 13 features identified on the supplemental investigative lead report to be considered for analysis. Review of the facial features and the corresponding morphological notes reveal the following:

- Four of the facial features ("Overall Head Shape", "Hairline", "Forehead/Brow Ridge", "Eyebrows") were noted to have been obstructed by the hat being worn by the suspect. Due to occlusions presented, these features would not have been used in the analysis.
- "Chin/Jawline" was stated to be "Obstructed by hair."
- The facial feature listed as the "Neck" was not visible for comparison.
- The "Ears" are listed as "not fully visible for comparison"; due to the angle of the face in the image, only one ear is visible at all, and it is not fully visible.
- The "Overall Face Shape" was noted to be "Partially obstructed by hat" but the report somehow concludes that the "Facial composition appears to be consistent."
- Only five of the facial features—"Eyes", "Nose", "Mouth", "Cheeks", "Facial Hair"—are listed with no note of an obstruction occurring and include some variation of the phrase of "appear to be consistent".

125. The phrase "appears to be consistent" should be used loosely. Given the "poor" image quality label indicated on the supplemental investigative lead report, there is no reason to conclude that any uniquely identified features are shared between the two photographs being compared.

126. In 2010, Klare and Jain proposed a taxonomy of facial features, codified into three levels, that could be used for automated and manual face recognition [15]. The capability of

today's AFR systems far exceeds the algorithms available in 2010. In my expert opinion, the taxonomy holds for manual comparisons performed by humans.

127. The taxonomy suggests that Level 1 features (i.e., IOD < 30 pixels) are sufficient for determining facial features such as skin tone, gender, and general appearance. Level 2 features (i.e., 30 pixels < IOD < 75 pixels) provide an analyst with the ability to locate and accurately measure ratios between key anthropometric landmarks (e.g., corners of the mouth, nose, eyes, etc.). And finally, Level 3 (IOD > 75 pixels) includes features such as moles, freckles, and skin discoloration.

128. I have estimated the IOD of the probe image of the suspect to be approximately 17-20 pixels. At this spatial resolution, there is not enough detail to locate and tag uniquely identifiable features shared between the persons being compared.

129. Without this level of detail, and given a poor-quality image to work with, it is highly unlikely that an analyst could provide a positive ID.

130. Additionally, there does not appear to be any objective measure used to determine what level of identifying measures are necessary for someone to qualify as an investigative lead. In this case, having some features in common with a person in a poor-quality probe image was enough to label a Mr. Williams as an investigative lead.

131. Therefore, the investigative lead report, as it should, explicitly states that "THIS DOCUMENT IS NOT A POSITIVE IDENTIFICATION. IT IS AN INVESTIGATIVE LEAD ONLY AND IS NOT PROBABLE CAUSE TO ARREST. FURTHER INVESTIGATION IS NEEDED TO DEVELOP PROBABLE CAUSE TO ARREST".

132. Further, law enforcement agencies have long been consistent in holding firm that face recognition search results are not used as positive identifications and are considered as

investigative leads only. For example, in 2017 the Department of Justice Bureau of Justice Assistance published a "Face Recognition Policy Development Template" which clearly states that that "Face recognition search results are not considered positive identification and do not establish probable cause, without further investigation; rather, they are advisory in nature as an investigative lead only. Any possible connection or involvement of an individual to a criminal investigation must be determined through further analysis and investigation" [16].

133. The photo of Mr. Williams was forwarded to an MSP supervisor for secondary analysis and approval to be sent to DPD. The entire gallery was *not* sent to the supervisor, only the probe photo and Mr. Williams's (expired) driver's license photo from the gallery. Four minutes after receiving the secondary analysis request, the supervisor provided a reply of "yes," after which the MSP analyst forwarded the photo to DPD as an investigative lead.

134. Upon receipt of the MSP investigative lead report, DPD CIU appears to have forwarded the investigative lead report to the lead detective, without assessing the quality of the match or providing a warning about the low likelihood of an accurate match based on the poor quality of the probe image. There is no testimony to indicate that DPD CIU asked MSP for any of the information discussed above that would have helped to assess the quality of the investigative lead. Nor is there evidence that MSP communicated any information that would have caused DPD detectives to feel confident in their abilities to take shortcuts in their investigation.

135. Without any additional investigation, the lead detective included the investigative lead in a photo array for a witness identification procedure.

136. In my expert opinion, DPD detectives should not have relied on the selection of Mr. Williams from the photo array by Ms. Johnston as cause to effect an arrest. Ms. Johnston was not an eyewitness to the crime and possessed no additional information as it pertains to the identity of the suspect beyond that of the MSP trained analyst. If standard operating procedures are that detectives are not to rely on an MSP-trained image analyst's ability to positively identify a suspect appearing in a poor-quality photo, it's concerning that DPD detectives would trust Ms. Johnston's ability to do so.

Summary

137. Face recognition technologies continue to proliferate and become deeper ingrained into our everyday lives. This technology is now used for logging into mobile phones, confirming passenger identification for air travel, and even more benign tasks such as organizing photos in a digital photo album. This in part is attributed to its ease of use and the impressive gains in accuracy in test conditions as documented in independent evaluations conducted by NIST.

138. Despite the gains in accuracy, there have been numerous articles published in mainstream media raising concerns over the use of face recognition technology by law enforcement and potential misidentifications of African Americans. These concerns were largely dismissed by law enforcement users of the technology. But to date, there are now five documented cases of wrongful arrests—all of which involve Black men [17]–[20]. And Mr. Williams was the first case involving an obvious wrongful arrest reported to the public at large.

139. It is difficult to understand how a detective charged with the responsibility of conducting a thorough investigation would fail to do so, given all the scrutiny and the many warnings being reported long before the arrest of Mr. Williams. It is even more challenging to

understand how an entire police department could allow its investigators to rely upon facial recognition technology without providing them with any training or background on how the technology works so that they could ask the questions necessary to determine how seriously to take an "investigative lead." The fact that DPD employs trained facial recognition analysts who also fail to ask any critical questions or provide necessary information to detectives suggests that the analysts either do not themselves understand how the technology functions and its possibility for generating false leads or else that they are indifferent to those risks.

140. There is no doubt that automatic face recognition is very *powerful* tool due its capacity to enable law enforcement to search through very large repositories—in this case 49 million records—in a matter of seconds/minutes for a subject appearing in an image or in a video media to generate a possible lead. But when detectives charged with investigating the lead produced using the AFR technologies fail to complete a very thorough and comprehensive analysis of supporting evidence, it becomes a very *dangerous* tool imposing grave risks to the everyday law-abiding citizens.

141. All evidence points to the fact that the DataWorks Plus system used by the Michigan State Police was configured for lead generation. In this configuration, there are no thresholds applied to ensure that a similarity score exceeds a set threshold prior to being promoted to the candidate list. The lead generation places the burden and trust on the analyst adjudicating the candidate list to eliminate any obvious errors; and investigators downstream in the process to unearth credible evidence needed to place the *"investigative lead"* at the scene of the crime prior to making contact and affecting an arrest.

142. Additionally, the quality of the photo of the suspect was rated as "*poor*" by the MSP analyst and insufficient to make a positive identification, either by the face recognition algorithms integrated into the DataWorks Plus System or by the MSP image analyst. Due to the low pixel count, shadows being cast on the face, and occlusions, it would have been challenging for even the top performing algorithms to generate a reliable match (i.e., similarity score high enough to be considered a legitimate match).

143. And despite the very clear and explicit disclaimer listed on the investigative lead report, detectives appear to have placed excessive weight on the investigative lead generated through the use of face recognition technology.

144. On the warrant request, the detective indicated that "Face recognition came back with a hit." Investigators should have learned during their hours of training, and it should be common knowledge in law enforcement that AFR technology is only used for investigative leads. And the characterization of the investigative lead produced using face recognition as "a hit" is a direct contradiction to the words clearly marked in bold red letters that this is not a positive identification.

145. In the end, the automatic face recognition did what it was configured to do. It was not configured to search only for a person with facial characteristics that matched the suspect. But instead, it was configured to search through a database containing 49 million images in a matter of seconds to retrieve images of people with facial features possessing attributes with some degree of similarity to the suspect for human adjudication.

146. The procedures that should have protected Mr. Williams, a law-abiding citizen, from this wrongful arrest were either non-existent or simply they failed.

If additional materials are provided to me in reference to this case, I reserve the right to supplement this report in the future.

Michael C. King, Ph.D.

May 26, 2023

Bibliography

[1] P. Grother, M. Ngan, and K. Hanaoka, “Face Recognition Vendor Test (FRVT) Part 2: Identification,” *NIST*, Sep. 2019, Accessed: May 19, 2023. [Online]. Available: https://www.nist.gov/publications/face-recognition-vendor-test-frvt-part-2-identification

[2] P. Grother, M. Ngan, and K. Hanaoka, “Face recognition vendor test part 3:: demographic effects,” National Institute of Standards and Technology, Gaithersburg, MD, NIST IR 8280, Dec. 2019. doi: 10.6028/NIST.IR.8280.

[3] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, “DeepFace: Closing the Gap to Human-Level Performance in Face Verification,” presented at the Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2014, pp. 1701–1708. Accessed: May 21, 2023. [Online]. Available: https://openaccess.thecvf.com/content_cvpr_2014/html/Taigman_DeepFace_Closing_the_2014_CVPR_paper.html

[4] “The Perpetual Line-Up,” *Perpetual Line Up*. https://www.perpetuallineup.org/ (accessed May 19, 2023).

[5] J. Buolamwini and T. Gebru, “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” in *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, PMLR, Jan. 2018, pp. 77–91. Accessed: May 21, 2023. [Online]. Available: https://proceedings.mlr.press/v81/buolamwini18a.html

[6] “‘Law Enforcement’s Use of Facial Recognition Technology.’” http://www.congress.gov/ (accessed Jan. 24, 2023).

[7] J. Lynch, “Hearing on Law Enforcement’s Use of Facial Recognition Technology”.

[8] S. Lohr, “Facial Recognition Is Accurate, if You’re a White Guy,” *The New York Times*, Feb. 09, 2018. Accessed: May 19, 2023. [Online]. Available: https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

[9] T. L. Johnson, N. N. Johnson, D. McCurdy, and M. S. Olajide, “Facial recognition systems in policing and racial disparities in arrests,” *Gov. Inf. Q.*, vol. 39, no. 4, p. 101753, Oct. 2022, doi: 10.1016/j.giq.2022.101753.

[10] K. K. S, K. Vangara, M. C. King, V. Albiero, and K. Bowyer, “Characterizing the Variability in Face Recognition Accuracy Relative to Race,” in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2019, pp. 0–0.

[11] K. Krishnapriya, V. Albiero, K. Vangara, M. C. King, and K. W. Bowyer, "Issues related to face recognition accuracy varying based on race and skin tone," *IEEE Trans. Technol. Soc.*, vol. 1, no. 1, pp. 8–20, 2020.

[12] H. Wu, V. Albiero, K. S. Krishnapriya, M. C. King, and K. W. Bowyer, "Face recognition accuracy across demographics: Shining a light into the problem," *ArXiv Prepr. ArXiv220601881*, 2022.

[13] "FRVT 1:N Identification." https://pages.nist.gov/frvt/html/frvt1N.html (accessed May 21, 2023).

[14] "Enhanced license and IDs." https://www.michigan.gov/sos/faqs/license-and-id/enhanced-license-and-ids (accessed May 17, 2023).

[15] B. Klare and A. K. Jain, "On a taxonomy of facial features," in *2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, Sep. 2010, pp. 1–8. doi: 10.1109/BTAS.2010.5634533.

[16] "Face Recognition Policy Development Template for State, Local, and Tribal Criminal Intelligence and Investigative Activities," Department of Justice's Office of Justice Programs, Dec. 2017. [Online]. Available: https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf

[17] "Wrongful arrest exposes racial bias in facial recognition technology," Nov. 19, 2020. https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/ (accessed May 24, 2023).

[18] K. Johnson, "Face Recognition Software Led to His Arrest. It Was Dead Wrong," *Wired*. Accessed: May 24, 2023. [Online]. Available: https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/

[19] K. Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," *The New York Times*, Dec. 29, 2020. Accessed: May 24, 2023. [Online]. Available: https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

[20] K. Hill and R. Mac, "'Thousands of Dollars for Something I Didn't Do,'" *The New York Times*, Mar. 31, 2023. Accessed: May 24, 2023. [Online]. Available: https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html

MICHAEL C. KING, Ph.D.

Phone: +1.703.598.6991
E-Mail: michaelking@fit.edu

EDUCATION

NORTH CAROLINA AGRICULTURAL AND TECHNICAL STATE UNIVERSITY, Greensboro, NC

Doctor of Philosophy in Electrical Engineering (August 2001)

- Dissertation: "Multi-Context Spoken Language Command Identification using Adaptive Neural Experts"
- *NASA Ronald E. McNair Doctoral Fellow*
- *Areas of Concentration: Computational Intelligence, Computer Networks, and Computer Vision.*

Master of Science in Electrical Engineering (December 1997)

- Thesis: "Pattern Recognition Using Parallel Neural Systems"
- *Areas of Concentration: Pattern Recognition and Power Systems*

Bachelor of Science in Electrical Engineering (December 1994)

NORTHWESTERN UNIVERSITY, Kellogg School of Management, Evanston, Il,

Certificate of Completion: The Innovative Organization (March 17-22, 2013)

- Topics: Action planning/crisis management, emotional intelligence, networking, teams, decision making, change implementation, and negotiations.

Clearance: *Top Secret / SCI*

SPONSORED RESEARCH

Total Contract Awards: ($13,114,196)

- **VIsual DOssiers for Recognizing & Identifying Humans at Altitude and Range (VIDORA),** Sponsor: IARPA; Role: Co-PI (University of Houston-Prime; Research partners: University of Houston, SRI, University of Toronto, Rank1 Computing, University of Miami, New Mexico State University, Teaq Innovations); PoP: November 2021 - September 2025; $2,901,000
- **Computational Psychology**, Sponsor: US Government; Role: PI (Florida Tech-Prime; Research partners: University of Pennsylvania, University of New Haven); PoP: July 2022 - December 2024; *Total Cost* $1,349,522
- **Automated Face Recognition Best Practices IV**, Sponsor: US Government; Role: PI (Florida Tech-Prime; Research partners: University of Notre Dame); PoP: March 2022 – June 2023; *Total Cost $405,000*
- **Automated Face Recognition Best Practices III**, Sponsor: US Government; Role: PI (Florida Tech-Prime; Research partners: University of Notre Dame); PoP: March 2021 - May 2022; *Total Cost $398,000*
- **Computational Psychology**, Sponsor: US Government; Role: PI (Florida Tech-Prime; Research partners: University of Pennsylvania, University of New Haven); PoP: July 2020 - December 2022; *Total Cost* $2,667,674
- **Automated Face Recognition Best Practices II**, Sponsor: US Government; Role: PI (Florida Tech-Prime; Research partners: University of Notre Dame); PoP: March 2020 - May 2021; *Total Cost $375,000*

- **Modelling plea decisions: Using computational science to enhance the impact of guilty-plea research,** Sponsor**:** American Psychology—Law Society; Role: Co-PI (Montclair State University-Prime; Partners: University of Exeter); *Total Cost: $26,350*
- **Cyber Identity and Behavioral Analytics Research (CIBAR) Consortium;** Sponsor: US Government; Role: PI (Florida Tech-Prime; Research partners: Auburn University, North Carolina A&T State University, UNC-Chapel Hill, UNC-Wilmington, University of Florida, Rutgers); Period of Performance: June 2018 - June 2021; *Total Funding $3,900,000*
- **Computational Psychology**, Sponsor: US Government; Role: PI (Florida Tech-Prime; Research partners: University of Pennsylvania, University of New Haven); PoP: July 2018 - May 2020; *Total Cost $550,000*
- **Automated Face Recognition Best Practices**, Sponsor: US Government; Role: PI (Florida Tech-Prime; Research partners: University of Notre Dame); PoP: March 2018 - December 2019; *Total Cost $355,000*
- **Multi-location Passenger Re-Identification,** Sponsor: Collins Aerospace; Role: PI; PoP: August 2018 - December 2019; *Total Cost $80,000*
- **Center for Advanced Studies in Identity Science**, Role: Co-PI (Lead Institution: North Carolina A&T State University); Sponsor: US Government; PoP: September 2017 - August 2018; *Total Cost $133,000*

Submitted/Awaiting Decision ($ 413,000)

- **Automated Face Recognition Best Practices IV**, Sponsor: US Government; Role: PI (Florida Tech-Prime; Research partners: University of Notre Dame); PoP: March 2023 – June 2024; *Total Cost $413,000*

PROFESSIONAL EXPERIENCE

FLORIDA INSTITUTE OF TECHNOLOGY, Melbourne, Fl. MD 8/15 – Present

Associate Professor, Department of Computer Engineering and Sciences
Research Scientist, Harris Institute for Assured Information

Courses Taught: Advanced topics in Computer Science—Cyber Identity; Biometric Authentication Technologies

CENTRAL INTELLIGENCE AGENCY (CIA), Washington DC 4/12 – 9/15

Directorate of Science and Technology / Advanced Research and Innovation Team
Director (9/14 – 9/15); Senior Scientist/Technical Director (10/13 – 9/14); Deputy Director (Acting: 6/13 – 10/13); Research Scientist (4/12 – 6-13)

Advance the CIA's mission through leadership in the development of strategic research and development roadmaps that address critical intelligence gaps in the technical areas of cyber, special communications systems, and identity intelligence.

- TECHNOLOGY LEADERSHIP: Leading a team of scientists and engineers in the development of a strategic research and innovation plan in response to the CIA's needs in Identity Intelligence.
- INTERAGENCY COORDINATION: Crafted Memorandum of Agreement with Government partner to formalize collaborative framework to drive research and innovation while facilitating the ease of technology transfer into Agency mission.
- DIVERSITY ADVOCATE: Secured funding to continue support of a CIA diversity outreach initiative in identity science at a Historically Black College or University (HBCU). Worked with mission offices to ensure research topics are aligned to impact future operational objectives. Sponsorship has also had a dramatic impact on diversity recruitment.

- TECHNICAL ADVISOR: Provide expert advice to senior leadership on resolution of scientific, technical, or program management issues; and technology investments to address mission imperatives.
- PROGRAM MANAGEMENT: Managing contract, personnel, and budget resources to direct research efforts in the area of identity intelligence and special communications. Certified as a Contracting Officer Technical Representative.

OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE, Washington DC 1/08 – 4/12

Intelligence Advanced Research Projects Activity (IARPA)
Program Manager (Joint Duty Assignment)

Tapped by Associate Director of National Intelligence for Science and Technology (ADNI S&T) to architect large-scale high-risk/high-payoff extramural research and development program in biometrics that significantly advances the IC's capabilities in Identity Intelligence.

- RESEARCH ADVOCATE: Campaigned senior IC officials to secure funding for large-scale R&D investment (i.e. tens of millions of dollars) to spur the advancement of biometrics technologies required to address critical challenges to the U.S. intelligence community.
- PROGRAM PLANNING: Directed team of scientists in the analysis of biometrics technology landscape to identify key capability gaps; resulted in the development of a strategic investment plan to drive revolutionary advancements in biometrics research. Formulated and implemented a 5-year / 3-phase research program plan, emphasizing programmatic integrity and technical excellence. Maximized the probability of success despite a high-degree of risk and uncertainty; served as the basis of the IARPA Biometrics Exploitation Science and Technology Program (BEST).
- PROPOSAL EVALUATION: Served as Chair, *Source Selection Evaluation Review Board*; presented consensus evaluation report to the Source Selection and Funding Authorities to support formulation of the BEST Program.
- PROGRAM MANAGEMENT: Provided technical direction and programmatic oversight for all aspects in Phase I (2 years) of the BEST Program (20+ contracts). Delivered advancements and bold innovation in biometric algorithms, exploitation system design, next generation sensor technology, and non-conventional optical systems. The Program covered face (including 3D), iris/ocular, and speaker recognition technologies. Teamed with the Army Research Laboratory (ARL) and Army Research Office (ARO) in the formulation, negotiation, and monitoring of contractual agreements.
- SCIENTIFIC LEADERSHIP: Promoted exploitation of periorbital (ocular) features as a complement to iris recognition technologies at the *IEEE International Conference on Biometrics: Theory, Applications, and System (2008)*; prompted more than 50 publications in this area. Authored "Afterword" for the "Handbook on Iris Recognition," which includes articles written by an international collection of scholars and a section on ocular recognition.
- RESEARCH COMMUNICATION: Chaired 4 technical conferences to promote cross-fertilization of ideas throughout the Program. Facilitated peer review and communicated advancements in the BEST Program to Government stakeholders; chaired 2 workshops.
- RESEARCH ADMINISTRATION: Provided high-level objectives and monitored task assignments of senior scientists charged with developing and executing test and evaluation plans. Assembled multi-disciplinary team of leading experts from multiple Government agencies (i.e. ARL, Army Night Vision, Department of Homeland Security (DHS), Federal Bureau of Investigations (FBI), United States Secret Service, and National Institute for Standards and Technology (NIST)) to serve as advisors on both technical and programmatic challenges.

- TECHNOLOGY TRANSFER & INTERAGENCY COORDINATION: Crafted interagency agreements to formalize strategic research partnerships with stakeholders ensuring research awareness and facilitating technology transfer. Successfully transitioned technology to more than 10 agencies/labs (e.g. IC, Department of Defense (DoD), and DHS).
- SENIOR OFFICIAL & CONGRESSIONAL ENGAGEMENT: Invited to brief the Director of National Intelligence 4 times in a 3-year period to communicate challenges facing the IC and development efforts in Identity Intelligence, and bolster support to increase funding levels for IARPA sponsored research programs.
- EXECUTIVE LEADERSHIP: Requested by ADNI S&T to continue to serve as the IC's Department Lead to the White House OSTP's NSTC Subcommittee on Biometrics and Identity Management. Represented interests paramount to the IC's 16 mission elements and provide authoritative guidance on the development of national policy as it pertains to the advancement and implementation of biometrics technology.

CENTRAL INTELLIGENCE AGENCY, Washington, DC 9/05 – 1/08

Directorate of Science and Technology / Intelligence Technology Innovation Center (ITIC)
Research Scientist / Program Manager (Joint Duty Assignment)

Invited by the IC's Chief Technology Officer to provide management and oversight of the IC's multi-million dollar biometrics research and development portfolio; served as principal advocate to secure funding for the development of biometrics technology; planned, analyzed and assessed the biometrics and identity science program for the IC, which includes the identification of new research initiatives and the integration of Government-wide research activities into the overall biometrics and identity science basic/applied research strategy and formulate new innovative program to address future IC operational requirements.

- EXECUTIVE LEADERSHIP: Continued to strengthen the IC's long-term research strategy for basic research in biometrics and identity science. Provided high-level vision and guidance for development of basic and applied scientific research programs aligned with broad-based IC mission imperatives for inclusion in the ITIC extramural research portfolio. Provided oversight and direction to experienced IC program managers executing 20+ projects/programs on behalf of ITIC. Provided authoritative guidance to resolve scientific and programmatic issues surfacing during the execution of the program.
- TECHNOLOGY TRANSFER: Initiated interagency coordination meetings with scientists and engineers from across Government agencies to discuss proposal submissions to assess relevance to the IC's mission. Actively monitored on-going projects to ensure the researchers' efforts are tied to IC research imperatives. Communicated research program activities and results to outside organizations to ensure that the basic research deliverables are transitioned to IC programs.
- PROGRAM EXECUTION: Initiated opportunity-driven basic research projects that contributed to ITIC's mission to exploit scientific opportunities for revolutionary new capabilities and to develop solutions to address existing IC challenges.
- PROJECT MANAGEMENT: Developed strategies and technical approaches to biometrics and identity science basic/applied research by engaging the scientific community. Identified, developed, and implemented opportunity-driven basic research projects with universities and private industry to support the ITIC's basic research program. Conducted technical meetings to discuss on-going ITIC-sponsored research contracts/cooperative agreements to promote and coordinate relationships between the IC and educational research institutions.
- EXECUTIVE LEADERSHIP: Appointed to serve as the IC's Department Lead to the White House OSTP's NSTC Subcommittee on Biometrics and Identity Management. Represented

interests paramount to the IC's 16 mission elements and provided authoritative guidance on the development of national policy as it pertains to the advancement and implementation of biometrics technology. Presented high-level R&D strategic objectives of the IC to facilitate coordination, leverage, and to de-conflict research projects across the Government (i.e. DoD, FBI, DHS, USSS, etc).

- RESEARCH ADVOCATE: Served as principal advocate to secure funding for the development of biometrics technology and formulate plans for a new innovative program, based on past experience, future IC customer operational needs, and a comprehensive survey of the commercial marketplace to identify strategic areas for investment.
- CONGRESSIONAL ENGAGEMENT: Provided multiple briefs to congressional staffers to promote research awareness and garner support for additional funding for initiatives conducted to address IC mission imperatives; selected by ADNI S&T to demonstrate an advanced biometrics capability for Congressional Representatives and staffers during the Intelligence Community Technology Expo on Capitol Hill. Project selected from a pool of applicants representing the most significant advancements across the IC.
- INTERAGENCY COORDINATION: Partnered with senior officials at OGAs (i.e. DoD, FBI, DHS, etc.) to sponsor the NIST Face Recognition Grand Challenge (FRGC) 2006, Face Recognition Vendor Test (FRVT) 2006, Iris Challenge Evaluation (ICE) 2006, and Multi-Biometric Grand Challenge (MBGC) 2008. Provided NIST program director with high-level vision to drive high-impact technology development in accordance with ITIC mission objectives.
- DIVERSITY ADVOCATE: Responded to the call of senior CIA officials to pilot an identity science outreach program with a Historically Black College or University (HBCU). Partnered with the ODNI Center of Academic Excellence Program and the ARL to establish the Center for Advanced Studies in Identity Science (CASIS); a consortium consisting of researchers from the North Carolina A&T State University, University of North Carolina at Wilmington, and Clemson University.
- RESEARCH COMMUNICATIONS: Documented and communicated the biometrics and identity science program emphasizing successes in funding extramural basic research IC to ensure awareness and aid in the transition of research outcomes into current and future IC systems. Supported principal investigators by providing leadership and consultation that ensured research efforts transition into current and future IC systems. Prepared scientifically sound summaries of significant accomplishments of on-going research efforts in the form of Weekly Activity Reports.

NATIONAL SECURITY AGENCY, Ft. Meade, MD 8/01 – 9/05

Research Directorate / Human Interface Security
Technical Director (9/02-9/05)

Identified, planned, and directed research activities to support the development of Identification and Authentication (IA) technologies to meet the needs of the DoD and the IC; served as SME in the area of biometric technologies for customers of the Information Assurance Research Office.

- STRATEGIC PLANNING: Crafted research development plans to provide vision, high-level objectives, and identify scientific opportunities of interest to guide formulation of research projects by staff researchers.
- TECHNICAL LEADERSHIP: Served as USG's lead scientist for proposal to the prestigious JASONs Defense Advisory Group on "*Intelligence Applications of Aspheric Optical Wavefront Coding.*" Successfully argued fundamental premise for proposal submission; subsequently selected for inclusion in the summer study program. Assembled and led a diverse team of expert scientists to provide support during the deep-dive period of the study.

- TECHNOLOGY LEADERSHIP/TRANSFER: Directed research that has led to the development of improved security in fingerprint sensors. Sensor uses spectroscopy to detect the presence of materials commonly used to spoof fingerprint recognition systems. Technology integrated with commercial fingerprint recognition systems to diffuse their vulnerability to common spoof attacks. Sensor has also been transitioned and deployed by Government user community.
- PROGRAM MANAGEMENT: Provided research program guidance and oversight in the areas of exotic sensors (w/free-space optics), anti-spoofable biometrics, face anthropometric morphological changes, remote assessment of human identity, and aspheric optics.
- RESEARCH ADVOCATE: Successfully formulated research proposals to secure external funding (i.e. tens of millions of dollars) from the IC's Advanced Biometrics Research portfolio manager in support of mission imperatives at NSA.
- CONTRACT MANAGEMENT: Served as Contracting Office Representative (COR) for biometrics and identity science/management related Indefinate Delivery Idefinate Quantity (IDIQ) task order. ($50M ceiling over a 5-year period.)
- TECHNICAL EXPERT: Served as SME in the review of proposals submitted to NSA's Biometrics Program and the ITIC biometric subgroup. Rated proposals on the criteria of technical merit, scope of work, schedule, and budget.
- RECRUITMENT: Supported recruitment projects by attending career fairs to serve as a technical recruiter. One of a select number of hiring advisors with authorization to grant "conditional job offers" to highly-qualified candidates.
- TECHNOLOGY LEADERSHIP: Served as Lead Engineer on the Virtual Secure Compartmented Information Facility (SCIF) pilot project for the Naval Security Group Command (CNSG). Demonstrated SCI-level information security and assurance by leveraging biometric technologies with integrated video motion analysis to build a secure environment without a traditional brick and mortar.
- RESEARCH COMMUNICATION: The concept prototype Virtual SCIF was selected as one of 6 project demonstrations showcased for VIP Guests at the National Security Agency's 2005 Research Associate Directorate Technology Expo, the DoD's 9th annual Information Assurance Workshop (February 2005, Philadelphia PA), and the DoD's Southern Command (June 2005, Miami, FL).
- STAFF DEVELOPMENT: Served as mentor for less experienced researchers and program managers; formulated performance evaluations and constructed professional development plans (training and conference attendance) for staff officers.
- CONGRESSION ENGAGEMENT: Briefed House Permanent Select Committee on Intelligence (HPSCI) and Senate Select Committee on Intelligence (SSCI) staffers on project areas pertaining to biometric identification and demonstrated an implementation of aspheric optics.

Signals Intelligence Directorate / Emerging Technologies
Global Network Exploitation Analyst (8/01-9/02)

Collaborated with team of engineering professionals to conduct a thorough analysis of emerging communication technologies to identify vulnerabilities and subsequently develop technology capable of exploiting emerging telecommunications networks.

- SOFTWARE DEVELOPMENT: Analyzed telecommunications systems and developed software capabilities to enable processing of targeted signals.
- COMMUNICATION: Assumed the role of course instructor for a portion of the emerging technologies section 2.5 months after joining the agency; course on exploiting emerging

telecommunication networks. Analysts attending this course acquired an understanding of the technical aspects of emerging technologies and exposed key indicators of use.

MORGAN STATE UNIVERSITY, Baltimore, MD 1/03 – 6/05

Department of Computer Science
Adjunct Professor
Courses: Intro/Advanced Network Communications and Computer Programming in C++.

NORTH CAROLINA A&T STATE UNIVERSITY, Greensboro, NC 2/97 – 8/01

Center for Computer Telephony Integration
Research Assistant
Researched application of Artificial Neural Networks to spoken language dialog to develop a modular neural system for the evolution of specialized neural components for context-dependent interaction.

- NETWORK ARCHITECH: Designed and implemented Asynchronous Transfer Mode (ATM) Network to provide toll grade telephony service over data network (Voice-over-ATM). The implementation provided OC-3 service to the desktop and OC-12 service across the ATM backbone, with a bridge to the campus area network. Provided Publicly Switched Telephone Network (PSTN) and remote access services via a fractionalized PRI-ISDN, using an ADTRAN Atlas 800 and a RasCom Server; served as network administrator for a network consisting of both 10/100 Ethernet and ATM (OC-3/OC12) equipment.
- RESEARCH: Utilized NeuralWorks Professional II and in-house software (C/C++) to solve pattern recognition problems with Soft Computing methodologies. Implemented Artificial Neural Networks on a SIMD Neural Array Processor (SNAP) to study the performance characteristics of parallel processing for solving high-dimensional feature space classification problems. Implemented a parallel-distributed genome splicing genetic algorithm in heterogeneous environment, using Parallel Virtual Machines.

MCNC, Research Triangle Park, NC 12/94 – 2/97

North Carolina Supercomputing Center
Software Engineer / Visualization Specialist
Provided key technical support in a team environment for the International Application Visualization System (AVS) Center, a vendor-sponsored user group for scientists and researchers using this modular visualization environment.

- DATA VISUALIZATION: Project Leader; utilized third-party software tools to design and develop (C, OpenGL) applications to enable visualization of large-scale scientific data in a virtual environment to demonstrate and assess the usability of the Vision Dome, a new virtual reality display technology.
- SOFTWARE ENGINEER: Key member of team; completed requirements and high-level design of a web-based High Performance Geographical Information System.
- CONSULTANT: Consulted on design and development of visualization techniques using AVS. Installed, tested, and maintained vendor and public domain visualization software.
- INFRASTRUCTURE SUPPORT: Designed, developed, and administered the public domain FTP/WWW site, consisting of 900+ modules; port public domain modules (C/C++, FORTRAN) to various hardware platforms and the next-generation AVS Object-Oriented Programming environment (AVS/Express).
- COMMUNICATION: Promoted and administered MCNC/AVS Campus Program to provide AVS licenses to educational institutions in NC. Demonstrated the use of AVS (AVS5.02 and AVS/Express) applications and conducted quarterly courses on scientific visualization.

Research Fellow / Principle Investigator (6/94 – 8/94)
Designed and developed interactive software system (C Language), Cardiac Arrhythmia Scientific Visualization Interface (CASVI 1.0) to study cardiac dynamics. The software tool links rapid number crunching ability of a CRAY-YMP Supercomputer to the high-powered rendering capabilities of a UNIX workstation.

DUKE UNIVERSITY, Durham, NC (Summers) 1992 – 1993
Engineering Research Center for Emerging Cardiovascular Technologies,
NSF / ERC Fellow (6/93 – 8/93)
Developed applications using AVS to study and visualize various forms of 3-D cardiac phenomena. Implemented the differential equations for the Fitzhugh-Nagumo model to simulate cardiac activation.

NSF / ERC Fellow (6/92 – 8/92)
Utilized AVS to visualize simulated volumetric data from large-scale excitations in cardiac tissue in 2-D and 3-D. Created an animation of the excitation and generated a video clip at the North Carolina Supercomputing Center, using the Abekus A60 video recorder.

HEWLETT PACKARD, Rohnert Park, CA 5/91– 8/91
Signal Analysis Division
Summer Internship/SEED Program
Worked in shipping and handling; documented the receiving process to ensure compliance with ISO 9000; Coded the LZW algorithm in TURBO-C to view GIF files.

NORTH CAROLINA A&T STATE UNIVERSITY, Greensboro, NC 2/91 – 12/94
Machine Intelligence and Power Associated Research Laboratory
Undergraduate Research Assistant (during academic semesters)
Evaluated implementation of Artificial Neural Networks on a SNAP to achieve real-time performance in the application areas of 3-D object recognition and computer vision. Evaluated the use of a gradient-based shape metric for recognizing 2-D objects. Collaborated on the design of an Expert System for Power System Planning and the development of the Graphical User Interface (C, Motif 1.1). Surveyed and analyzed power system stability using Power Flow programs.

HONORS AND AWARDS

ODNI Service Award (2012)
Joint Duty Award (2010)
ODNI Certificate of Distinction (2009)
Promotion – GS 15 (2008)
Intelligence Community Assignment Completion Award (2008)
NSA Service Award (2008)
Promotion – GS 14 (2005)
Numerous other lower-level letters/certificates of appreciation and recognition from DoD, the Executive Office of the President, IARPA, NSA, FBI, and ODNI.

INTERAGENCY BRIEFINGS (Select)

Biometrics & Identity Intelligence

- 3rd Annual USG Face Recognition Collaboration Meeting, sponsored by the Federal Bureau of Investigations Biometric Center of Excellence (February 2012)
- Department of Defense Science & Technology Biometrics and Forensics, Research Development Test & Evaluation Forum (August 2011)
- Department of Homeland Security Biometrics Coordination Group (May 2011)
- Federal Bureau of Investigations Biometrics Steering Committee (April 2011)
- Department of Justice Biometrics Workshop (February 2011)
- Department of Defense Science & Technology Forum (July 2010)
- Army Science Board study on Non-cooperative Biometrics (May 2010)

CONTRIBUTOR AND/OR REVIEWER

Publications by White House OSTP National Science and Technology Council's
Subcommittee on Biometrics and Identity Management

- The National Biometrics Challenge, September 2011
- Biometrics in Government Post- 9/11: Advancing Science, Enhancing Operations, August 2008
- National Security Presidential Directive-59/Homeland Security Presidential Directive-24, "Biometrics for Identification and Screening to Enhance National Security," June 2008
- Privacy and Biometrics: Building a Conceptual Foundation, September 2006
- The National Biometrics Challenge, August 2006

SELECT INVITED SEMINARS/PANELS

- "Characterization of Face Recognition Relative to Gender Mis-Classification"; Auburn University, November 2021
- "The Relationship of Face Recognition on Gender Classification;" (Face Recognition Workshop)—Federal Id, Washington DC, August 2021
- "Face Recognition Accuracy Relative to Race and Gender Demographics"; Oak Ridge National Laboratory, April 2021
- WEDU PBS Community Cinema – "Coded Bias" – Panelist, March 2021
- "Demographic effects in face recognition", Biometrics Institute US Conference, Washington DC, March 2020
- "Technology: Myths, Reality & Likely Future Performance of Face Recognition", Connect ID, Washington DC, March 2020
- IEEE Ethics in technology Panel
- "Bias in Face Recognition Performance", NSF Sponsored Bias in AI Workshop, Rutgers University, September 2019

- "Demographic Effects of Race on Face Recognition", Idemia User Group Conference, San Diego, CA, June 2019
- "Demographic Variations in Face Recognition Performance", United Technologies Research Corporation, April 2019
- "Demographic Effects of Race on Face Recognition Performance", Intelligence Advanced Research Projects Activity, April 2019
- "Demographic Variations in Face Recognition Performance", University of Houston, March 2019
- "Cyber Identity and Demographic Effects of Race on Face Recognition Performance" Alcorn State University, March 2019
- "Bias in Face Recognition, What's all the fuss"; National Press Club, Washington DC, December 2018
- "Face Recognition Performance Variations Due to Race", NIST International Conference on Face Recognition, November 2018
- "Cyber Identity and Behavioral Analytics", University of Auburn, October 2018
- "Identity Data in Cyber", Idemia User Group Conference, Alexandria VA, June 2017
- "Identity Attributes Discoverable in Cyberspace", Wilmington Information Technology Exchange, Wilmington, NC April 2017
- "The face: Moving beyond face recognition to facial analytics", International Conference on Biometrics and Identity, London, England, October 2015
- "Advanced Biometrics Research and the Intelligence Community," Intelligence, Surveillance, and Reconnaissance Systems and Technology Workshop, MIT Lincoln Laboratory, October 2011
- "Robust Biometrics Exploitation Science and Technology," International Joint Conference on Biometrics, September 2011
- "The Intelligence Advanced Research Projects Activity: Its BEST and Beyond," Conference of Lasers and Electro-optics, May 2011
- "BEST Speaker Recognition Research, Spoken Language Technology and Applications Workshop, MIT Lincoln Laboratory, December 2008
- "The Science of Biometrics Research with Relaxed Constraints, 2nd Annual IEEE International Conference on Biometrics Theory Applications and Systems, September 2008
- "Advanced Biometrics Research: An IC Perspective, 1st IEEE International Conference on Biometrics Theory Applications and Systems, September 2007

TECHNICAL CONFERENCES / WORKSHOP ACTIVITIES

- Program C0-Chair, 4rd Workshop on Demographics in Biometrics, IEEE Winter Applications in Computer Vision, January 2023
- Program Co-Chair, Co-organizer: Understanding and Mitigating Demographic Bias in Biometric Systems, IEEE International Conference on Pattern Recognition, 2022
- Program Chair, 3rd Workshop on Demographics in Biometrics, IEEE Winter Applications in Computer Vision, January 2022
- Co-chair, Special Session, International Joint Conference on Biometrics, September 2020
- Session Chair, IEEE Winter Applications in Computer Vision, March 2020
- Program Chair, 2nd Workshop on Demographics in Biometrics, IEEE Winter Applications in Computer Vision, March 2020
- Program Chair, 1st Workshop on Demographics in Biometrics, IEEE Winter Applications in Computer Vision, TBH January 2019

- Panel Chair, "Biometric Face Recognition and Privacy", Connect ID, Washington DC, May 2018
- Panel Chair, "FRONTIERS IN RESEARCH AND INNOVATION," Biometrics Congress, London UK., Nov 2017
- Panel Chair, "Big Data, Big Decisions: How enterprises are leveraging big data to make better informed decisions," Tech Beach, Montego Bay Jamaica, Nov 2017
- Technical Program Committee, International Conference on Biometrics, June 2016
- IARPA Biometrics Exploitation Science and Technology 3rd Principle Investigator's Conference, Las Vegas, NV, December 2011 (Chair)
- IARPA Biometrics Exploitation Science and Technology 2nd Principle Investigator's Conference, Charlotte, NC, June 2011 (Chair)
- IARPA Biometrics Exploitation Science and Technology 1st Principal Investigator's Conference, San Diego, CA, August 2010 (Chair)
- IARPA Novel Biometrics Workshop, College Park, MD, March 2010 (Chair)
- Panel Discussion: Advancements in Biometrics Technologies, National Counterintelligence Executive Workshop in Emerging Technologies, December 2008
- Robust Biometrics: Understanding Science and Technology, Honolulu, HI, November 2008 (Organizing Committee)
- Moderator: Advanced Biometrics Session, Biometrics Consortium Conference, September 2006
- Moderator: Advanced Biometrics Session, Biometrics Consortium Conference, September 2005

PUBLICATIONS

- A. E. E. Gbekevi, P. Vela, G. Pangelinan, M. C. King, and K. W. Bowyer, "Analyzing the Impact of Gender Misclassification on Face Recognition Accuracy," in Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, 2023, pp. 332–339.
- A. Bhatta, V. Albiero, K. W. Bowyer, and M. C. King, "The Gender Gap in Face Recognition Accuracy Is a Hairy Problem," in Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, 2023, pp. 303–312.
- H. Wu, G. Bezold, M. Günther, T. Boult, M. C. King, and K. W. Bowyer, "Consistency and Accuracy of CelebA Attribute Values," ArXiv Prepr. ArXiv221007356, 2022.
- V. Albiero, K. W. Bowyer, and M. C. King, "Face Regions Impact Recognition Accuracy Differently Across Demographics," in 2022 IEEE International Joint Conference on Biometrics (IJCB), 2022, pp. 1–9.
- H. Wu, V. Albiero, K. S. Krishnapriya, M. C. King, and K. W. Bowyer, "Face recognition accuracy across demographics: Shining a light into the problem," ArXiv Prepr. ArXiv220601881, 2022.
- Krishnapriya, KS; Pangelinan, Gabriella; King, Michael C; Bowyer, Kevin W; "Analysis of Manual and Automated Skin Tone Assignments for Face Recognition Applications", Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision Workshops, 2022
- Qiu, Ying; Albiero, Vítor; King, Michael C; Bowyer, Kevin W; "Does Face Recognition Error Echo Gender Classification Error?", Proceedings of the IEEE International Joint

conference on Biometrics, 2021

- Michel, Kay; Smith, Marcellus; Brown, Brandon; King, Michael; Dozier, Gerry; "A Study of Social Network Messages During the COVID-19 Infodemic: Salient Features and the Propagation of Information Types", SoutheastCon 2021, 1-8, 2021 IEEE
- Smith, Marcellus; Brown, Brandon; Dozier, Gerry; King, Michael; "Mitigating Attacks on Fake News Detection Systems using Genetic-Based Adversarial Training" 2021 IEEE Congress on Evolutionary Computation (CEC) , 1265-1271, 2021 IEEE
- Albiero, Vítor; Bowyer, Kevin; Vangara, Kushal; King, Michael; "Does face recognition accuracy get better with age? deep face matchers say no", Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, 261-269 2020
- Albiero, Vitor; KS, Krishnapriya; Vangara, Kushal; Zhang, Kai; King, Michael C; Bowyer, Kevin W; "Analysis of gender inequality in face recognition accuracy", Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision Workshops, 81-89, 2020
- Krishnapriya, KS; Albiero, Vítor; Vangara, Kushal; King, Michael C; Bowyer, Kevin W; "Issues related to face recognition accuracy varying based on race and skin tone", Transactions on Technology and Society, 1 1, 8-20, 2020, IEEE
- Bowyer, Kevin W; King, Michael C; Scheirer, Walter J; Vangara, Kushal; "The "Criminality From Face" Illusion", IEEE Transactions on Technology and Society, 1 4, 175-183, 2020
- Allred, Jordan; Packer, Sadaira; Dozier, Gerry; Aykent, Sarp; Richardson, Alexicia; King, Michael C; "Towards a Human-AI Hybrid for Adversarial Authorship", 2020 SoutheastCon, 1-8 2020
- Richardson, Alexicia; Dozier, Gerry; King, Michael C; Chapman, Richard; "'Uh-oh Spaghetti-oh': When Successful Genetic and Evolutionary Feature Selection Makes You More Susceptible to Adversarial Authorship Attacks" 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 567-571 , 2020
- Smith, Marcellus; Richardson, Alexicia; Brown, Brandon; Dozier, Gerry; King, Michael; Morris, Joshua; "A study of the impact of evolutionary-based feature selection for fake news detection", 2020 IEEE Symposium Series on Computational Intelligence (SSCI), 1859-1865, 2020
- Brown, Brandon; Richardson, Alexicia; Smith, Marcellus; Dozier, Gerry; King, Michael C; "The Adversarial UFP/UFN Attack: A New Threat to ML-based Fake News Detection Systems?" 2020 IEEE Symposium Series on Computational Intelligence (SSCI), 1523-1527, 2020
- Torres, Giordano Benitez; King, Michael C; "Harvesting Faces from Social Media Photos for Biometric Analysis", 2020 IEEE International Symposium on Technology and Society (ISTAS), 230-234 2020
- S, Krishnapriya K; Albiero, Vitor; Vangara, Kushal; King, Michael C; Bowyer, Kevin; "Differences in Face Recognition Accuracy Related to Race and Skin Tone", IEEE Transactions on Technology and Society On page(s): 0 Print ISSN: 2637-6415 Online ISSN: 2637-6415 Digital Object Identifier: 10.1109/TTS.2020.2974996, 2020
- Albiero, Vitor, Krishnapriya KS, Kushal Vangara, Kai Zhang, Michael C. King, and

Kevin W. Bowyer. "Analysis of gender inequality in face recognition accuracy." In Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision Workshops, pp. 81-89. 2020.

- Albiero, Vítor, Kevin Bowyer, Kushal Vangara, and Michael King. "Does face recognition accuracy get better with age? deep face matchers say no." In Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, pp. 261-269. 2020.
- Bowyer, Kevin; King, Michael C; "Why face recognition accuracy varies due to race", Biometric Technology Today, Elsevier Advanced Technology, 2019
- Michel, Mary C Kay; King, Michael C; Cyber Influence of Human Behavior: Personal and National Security, Privacy, and Fraud Awareness to Prevent Harm 2019 IEEE International Symposium on Technology and Society (ISTAS), 2019
- S, Krishnapriya K; Vangara, Kushal; King, Michael C; Albiero, Vitor; Bowyer, Kevin; "Characterizing the Variability in Face Recognition Accuracy Relative to Race", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2019
- Srinivas, Nisha; Ricanek, Karl; Michalski, Dana; Bolme, David S; King, Michael; "Face Recognition Algorithm Bias: Performance Differences on Images of Children and Adults", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops 2019
- Srinivas, Nisha; Hivner, Matthew; Gay, Kevin; Atwal, Harleen; King, Michael; Ricanek, Karl; "Exploring Automatic Face Recognition on Match Performance and Gender Bias for Children", 2019 IEEE Winter Applications of Computer Vision Workshops (WACVW), 2019
- Michel, Mary C Kay; King, Michael C; "The Future of Cyber Analytics: Identity Classification for Systematic and Predictive Insight", 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2019
- J Gaston, M Narayanan, G Dozier, DL Cothran, C Arms-Chavez, M Rossi, MC King, J Xu, "Authorship Attribution via Evolutionary Hybridization of Sentiment Analysis, LIWC, and Topic Modeling Features", 2018 IEEE Symposium Series on Computational Intelligence (SSCI), 933-940, 2018
- J Gaston, M Narayanan, G Dozier, DL Cothran, C Arms-Chavez, M Rossi, MC King, J Xu, "Authorship Attribution vs. Adversarial Authorship from a LIWC and Sentiment Analysis Perspective" 2018 IEEE Symposium Series on Computational Intelligence (SSCI), 920-927
- M Narayanan, J Gaston, G Dozier, L Cothran, C Arms-Chavez, M Rossi, MC King, K Bryant "Adversarial Authorship, Sentiment Analysis, and the AuthorWeb Zoo" 2018 IEEE Symposium Series on Computational Intelligence (SSCI), 928-932
- MK Michel, MC King, "Towards An Adaptable System-based Classification Design for Cyber Identity" 2018 International Conference On Cyber Situational Awareness, Data Analytics
- MC Michel, MC King, "Categorization of Discoverable Cyber Attributes for Identity Protection, Privacy, and Analytics" SoutheastCon 2018, 1-5 1 2018

- C Faust, G Dozier, J Xu, MC King, “Adversarial authorship, interactive evolutionary hill-climbing, and author CAAT-III” 2017 IEEE Symposium Series on Computational Intelligence (SSCI), 1-8
- M. C. King, “Afterword”, Handbook of Iris Recognition, 2013
- E. Patterson, A. Sethuram, M. Albert, K. Ricanek, M. King, “Aspects of Age Variation in Facial Morphology Affecting Biometrics,” 1st IEEE International Conference on Biometrics Theory Applications and Systems, Crystal City, VA 2007
- K. N. Smith, V. P. Pauca, A. Ross, T. Torgersen, M. C. King, “Extended evaluation of simulated wavefront coding technology in iris recognition,” 1st IEEE International Conference on Biometrics Theory Applications and Systems, Crystal City, VA 2007
- M. C. King, G. L. Lebby, and K. Ricanek, “A Dialog Control Strategy Using A Hierarchical Controller of Mutually Exclusive Neural Experts,” IASTED International Conference on Artificial Intelligence and Soft Computing, Cancun, Mexico, 2001
- M. C. King, S. L. Bryson, G. L. Lebby and A. Kumoluyi, “A Genome Splitting Algorithm For High Dimensional Feature-Space Classifier System Design,” IASTED International Conference on Artificial Intelligence and Soft Computing, Honolulu, Hawaii, 1999
- “*Computational Linguistics,”* Session Co-Chair, IASTED International Conference on Artificial Intelligence and Soft Computing, Honolulu, Hawaii, August 9th-13th, 1999
- M. C. King and G. L. Lebby, "Pattern Recognition using Parallel Neural Systems", IASTED International
- Conference on Artificial Intelligence and Soft Computing, Cancun, Mexico, 1998.
- M. C. King, G. L. Lebby, and A. Homaifar, "Feature Selection for Multi-Class Learning Tasks", Presented at the NASA URC Conference, Huntsville, Alabama, 1998
- "*AVS in Medicine,*" Panel Chair, AVS '95 User Group conference, Boston Massachusetts, March 1995
- K. Bullock et al., "An Automated Technique For Identification And Analysis Of Activation Fronts In A 2-D Electrogram Array," Computers in Biomedical Research, May 1994
- M. J. Cooke, M. C. King and G. L. Lebby, "A Generalized Regression Neural Network For Optimal Control Signal Generation," 1st Annual HSCTV conference, December 1994
- M.C. King and G. L. Lebby, "Multivariable Function Interpolation Using A GMDH Network," Proc. of the 24th Annual Southeastern Symposium on System Theory, March 1992

GRADUATE STUDENTS

Doctoral

- Advisor: Kushal Vangara (Florida Institute of Technology, PhD student, Computer Science, expected graduation 2022)
- Advisor: Gabriella Pangelinan (Florida Institute of Technology, PhD Student, Computer Science, expected graduation 2025)
- Advisor: Praveen Kumar (Florida Institute of Technology, PhD Student (part-time), Computer Science, expected graduation 2026)
- Advisor: Krishnapriya K. Sugouthan (Florida Institute of Technology, PhD Computer Science, May 2021)
- Advisor: Mary Michel (Florida Institute of Technology, PhD Computer Science, May 2020)
- Committee member: Kholud Alghamdi (Florida Institute of Technology, PhD student Computer Science)

- Committee member: Josemar Faustino Da Cruz (Florida Institute of Technology, PhD Computer Science, Dec 2019)
-

Doctoral (Partner Universities)

- Committee member: Brandon Brown (Auburn University, Computer Science)
- Committee member: Sadaira Packer (Auburn University, Computer Science)
- Committee member: Marcellus Smith (Auburn University, Computer Science, 2022)
- Committee member: Vitor Albiero (University of Notre Dame, Computer Science, 2022)

Masters

- Advisor: Paloma Vela (Florida Institute of Technology, MS/ Computer Science, Expected graduation, May 2022)
- Advisor: Brandon Ledford (Florida Institute of Technology, MS Information Assurance and Cyber Security, Expected December 2021)
- Advisor: Afi Edem-Edi Gbekevi (Florida Institute of Technology, MS Information Assurance and Cyber Security, August 2021)
- Advisor: Rosalin Dash (Florida Institute of Technology, MS Computer Science, August 2020)
- Advisor: Giodano Benitez (Florida Institute of Technology, MS Information Assurance and Cyber Security, Dec 2019)
- Advisor: Prasad Garapati (Florida Institute of Technology, MS Information Assurance and Cyber Security, Dec 2018)
- Advisor: Kushal Vangara (Florida Institute of Technology, MS Information Assurance and Cyber Security, May 2018)
- Advisor: Praveen Kumar (Florida Institute of Technology, MS Information Assurance and Cyber Security, Dec 2016)
- Committee Member: Leena Alghamdi (Florida Institute of Technology, MS Information Assurance and Cyber Security, May 2020)
- Committee Member: Kelly Smith (West Virginia University, MS Electrical Engineering, 2007)

IC Government Postdoctoral Fellows

- Government Technical Advisor; Dr. Lauren Kennell (United States Naval Academy, Intelligence Community Post-Doctoral Research Fellow, 2007)
- Government Technical Advisor; Dr. Damon Woodard (University of Notre Dame, Intelligence Community Post-Doctoral Research Fellow, 2006)