OHIO ATTORNEY GENERAL FACIAL RECOGNITION TASK FORCE

REPORT & RECOMMENDATIONS

JANUARY 26, 2020

TABLE OF CONTENTS

APPENDICES

ATTACHMENTS

EXECUTIVE SUMMARY

Ohio Attorney General Dave Yost empaneled a Task Force to review Ohio's facial recognition database that met for the first time on September 23, 2019. The Task Force charge was to advise the attorney general's office on how to operate Ohio's facial recognition system as an effective tool for law enforcement while protecting privacy and civil liberties. Members of the Task Force include civilian technology experts and many of the members have or do serve on Ohio Law Enforcement Gateway (OHLEG) Steering Committee established per Ohio Revised Code Section 109.57[i] or the OHLEG Advisory Committee.

The Task Force met eight times in the months of October 2019 – January 2020. The first meeting agenda discussion topics guided content for future meetings. The discussion topics outlined were:

Level of Access to Law Enforcement:
- Should all facial recognition searches be run through the Bureau of Criminal Identification and Investigation (BCI) or should law enforcement have direct access to the facial recognition database?
- What training requirements should be in place to utilize the facial recognition database?

Facial Recognition Database Update:
- Should BMV and BCI work to include the new, standardized photos into the facial recognition database? How often should this occur?
- Is there a privacy right for citizens in their drivers' license or identification card picture? If so, how far does this right extend?

Racial & Gender Concerns:
- What factors impact the accuracy and reliability of facial recognition technology, such as race or gender difference? How can Ohio's facial recognition system account for these shortcomings in practice?

Best Technology:
- How does Ohio's facial recognition system compare to industry standards?

Two meetings of the Task Force included subject matter expert presentations, specifically on November 19, 2019, Clare Garvie[ii], Senior Associate, Center of Privacy and Technology at Georgetown University and on December 3, 2019 a demonstration via WebEx from NEC[iii], the vendor selected by the Ohio Attorney General's Office to transition the facial recognition database system to a new platform (expected March 2021).

The Task Force recognized and often repeated that the use of facial recognition technology for law enforcement is an *investigative tool*. The Task Force was further guided by its interest in building public trust and confidence in the system while enhancing public safety. As such, it was understood that the Task Force would assist the Attorney General in identifying ways to improve training standards, rules, transparency and safeguards to prevent abuses of the facial recognition database. The business of the Task Force was conducted by an attempt to achieve majority consensus of members present (in person or by phone conference) regarding the discussion topics.

Thus, what follows are general recommendations regarding the oversight and administration of the facial recognition database, including: who should have access to the database; what images should be in the database; how to monitor, audit and improve transparency of the database; and resources identified as best practices for

future policy development. We must anticipate the advancement of technology and our goal is to facilitate its use in a way that enhances public safety while building public trust and confidence by:

Recommendation #1

The Ohio Attorney General should appoint a Facial Recognition Advisory Committee to work in collaboration with the OHLEG Advisory Committee and to assist the OHLEG Steering Committee.

Recommendation #2

The General Assembly should be encouraged to weigh-in on the appropriate use of Facial Recognition technology and its oversight.

Recommendation #3

The Attorney General should limit access to the Facial Recognition database to trained professionals at the Bureau of Criminal Investigation.

Recommendation #4

The Attorney General should declare a moratorium on the use of "live" facial recognition.

Recommendation #5

The Attorney General should maintain the current OHLEG standard that expressly prohibits the use of facial recognition to conduct surveillance of persons or groups based solely on their religious, political, or other constitutionally protected activities or affiliations.[iv]

Recommendation #6

The Attorney General should promulgate a specific standard for when law enforcement may utilize facial recognition and define investigative purpose for its use. This standard should require reasonable suspicion that the person to be identified has committed a crime, the person's actions present a danger to human life or may cause serious physical harm, or that law enforcement must use facial recognition to identify someone who is not able to identify him or herself.

Recommendation #7

The Attorney General should follow the recommended guidance from the Facial Identification Scientific Working Group (FISWG)[v] ***for security and maintenance of the system.***

Recommendation #8

The Attorney General should follow the recommended guidance from the National Institute of Standards and Technology (NIST)[vi] ***to conduct accuracy assessments of how the system works.***

Recommendation #9

The facial recognition database system should have an image quality standard and disqualify images that do not meet that standard.

Recommendation #10

Probe images used by law enforcement should not be enrolled in the facial recognition database.

Recommendation #11

The Attorney General should seek agreement from the Department of Public Safety and Bureau of Motor Vehicles (BMV) to enroll current BMV images that meet the requisite image quality standard in the facial recognition database.

Recommendation #12

Ohio's Facial Recognition Policy should address routine monitoring, periodic audits, enforcement, and public transparency.

Recommendation #13

The Attorney General should ensure the public has access to information about the use and regulation of facial recognition in Ohio.

TASK FORCE MEMBERS*

- Sara Andrews, Director, Ohio Criminal Sentencing Commission, Chair
- John Eklund, Ohio Senate
- Jeff LaRe, Ohio House of Representatives
- Paula Hicks-Hudson, Ohio House of Representatives
- Forrest Thompson, Prosecutor, Medina County
- Patrick Clark, Asst. State Public Defender, Ohio Public Defender's Office
- Anne Dean, Assistant Registrar, Ohio Bureau of Motor Vehicles
- Judge Matthew Reger, Wood County Court of Common Pleas
- Terri Enns, Professor, The Ohio State University and member, ACLU Ohio
- Dennis Hirsch, Professor, The Ohio State University Moritz College of Law and Capital University Law School
- Joel King, Jr., NAACP
- Larry Price, Elder, NAACP
- Peter Glenn-Applegate, Asst. U.S. Attorney, U.S. Dept. of Justice
- Tom Stein, Deputy General Counsel, CLEAR
- Steve Robinette, Councilman, City of Grove City
- Monica Moll, Ph.D., Director of Public Safety, The Ohio State University
- Brian DiMasi, Senior Corporate Counsel, Safelite Auto Glass
- Jeremy Hansford, IT Manager, Ohio State Highway Patrol
- Brian Ray, Professor, Cleveland-Marshall College of Law
- Phil Stammitti, Sheriff, Lorain County
- Timothy Pierce, Appellate Unit Chief, Franklin County Public Defender's Office
- Judy Wolford, Pickaway County Prosecutor
- Carol O'Brien, Deputy Atty. General for Law Enforcement & Chief Counsel, Ohio Atty. General's Office
- Joseph Morbitzer, Superintendent, Atty. General's Office's BCI
- Heinz von Eckartsberg, Asst. Superintendent, Atty. General's Office's BCI
- Beth Owens, Director of Identification, Atty. General's Office's BCI
- Jill Small, OHLEG Director, Atty. General's Office's BCI
- Lisa Sprague, Atty. General's Office's BCI
- Douglas Dumolt, Director of Law Enforcement Operation, Ohio Atty. General's Office

* Level and type of member participation varied throughout the work of the Task Force. Each member was afforded opportunity to participate in person, phone conference or email correspondence. Member participation is not unqualified endorsement of the Task Force final recommendations.

RECOMMENDATIONS

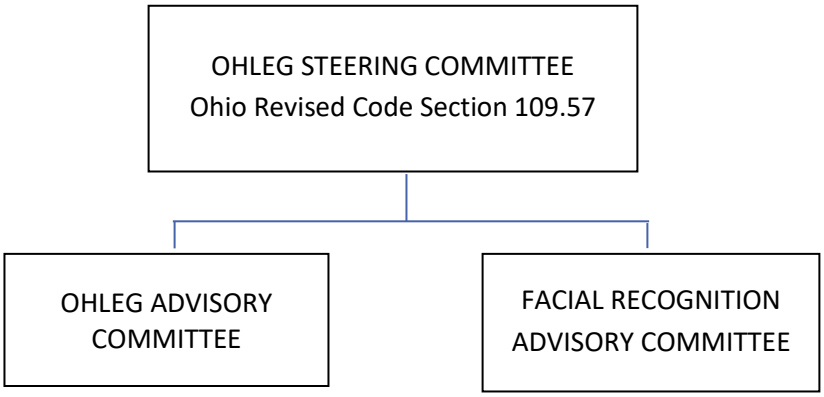
A. Oversight and Guidance

Recommendation #1

The Ohio Attorney General should appoint a Facial Recognition Advisory Committee to work in collaboration with the OHLEG Advisory Committee and to assist the OHLEG Steering Committee.

In 2013 the Ohio Law Enforcement Gateway (OHLEG) Steering Committee and OHLEG Advisory Committee were established per Ohio Revised Code Section 109.57. The primary duties of the OHLEG Steering Committee are to review, monitor and update the OHLEG and facial recognition policies. The OHLEG Advisory Committee is made up of professionals from a broad range of agencies who assist the OHLEG Steering Committee as policies are developed.

Because facial recognition technology is a powerful tool, evolving at a rapid pace the Task Force believes it is necessary to create the Facial Recognition Advisory Committee to examine how the system can be used as an effective tool for law enforcement while also maintaining the public's privacy and protecting civil liberties. The Facial Recognition Advisory Committee should also recommend training requirements that include making users aware of the system's limitations, such as current software's inadequacy in correctly identifying women and African-Americans and identify best practices and safeguards going forward.



Recommendation #2

The General Assembly should be encouraged to weigh-in on the appropriate use of Facial Recognition technology and its oversight.

Throughout the work of the Task Force there were conversations about and reports of legislatures, city administration and others with law or rule making authority proposing ways to prohibit, regulate and monitor the use of facial recognition technology. Reports including the *Perpetual Line-Up* encourage Congress and state legislatures to pass commonsense laws to regulate law enforcement use of facial recognition technology.[vii]

B. Access to the Facial Recognition Database

Recommendation #3
The Attorney General should limit access to the Facial Recognition database to trained professionals at the Bureau of Criminal Investigation.

Ohio's facial recognition technology is strictly controlled through OHLEG[viii], which provides criminal justice agencies access to a wide variety of databases containing information vital to the investigation of crime and missing persons. One of those databases is the facial recognition database.[ix] In August 2019, access to the database was reduced to a small number of employees at the Bureau of Criminal Investigation (BCI) to conduct facial recognition searches.

The Task Force spent considerable time contemplating this recommendation and ultimately agreed that recommending a centralized process for access to the database provides advantages that mitigate risks associated with the use of facial recognition technology. Those advantages include: increased quality of searches by trained investigators, a curated culture of appropriate use, clear accountability, demonstrated consistency, attentive safeguards, and improved public confidence. The implementation of a centralized process will necessitate operational and policy considerations like hours of availability and protocol for high risk or emergency situations.

A centralized process also provides opportunity to improve training standards in anticipation of new software. Current training standards are premised on what will become a legacy system and rely on an acknowledgment of participation. Prospective training standards should incorporate proficiency standards, development of an investigator manual, and consider a peer review process. The development of those standards should be guided by credible, recognized best practices.

Thus, the Task Force suggests BCI consider mandatory training that is recommended or provided by the Facial Identification Scientific Working Group (FISWG)[x] or the Federal Bureau of Investigation, Criminal Justice Information System Division (CJIS)[xi].

The Task Force supports maintaining the current OHLEG standard for federal agency access.[xii]

C. Facial Recognition System Use

Recommendation #4
The Attorney General should declare a moratorium on the use of "live" facial recognition.

The discussions of the Task Force surrounding the types of use of facial recognition focused on how best to craft useful recommendations to balance people's privacy interests with the need for public safety. The Task Force defined live facial recognition as identifying people in a video in real time, using a set of photographs as a reference or camera scanning a crowd for matches between members of the public and the people in the database.

There was general agreement that the power of facial recognition technology could have a dangerous chilling effect for the public if it were misused. Further, research has demonstrated its inaccuracies for identifying darker-

complexion and female faces. Therefore, after considering the potential impact on privacy, civil liberties, civil rights and the Task Force recommends the moratorium on the use of live facial recognition.

Recommendation #5

The Attorney General should maintain the current OHLEG standard that expressly prohibits the use of face recognition to conduct surveillance of persons or groups based solely on their religious, political, or other constitutionally protected activities or affiliations.[xiii]

In 2016, researchers from the Georgetown Law, Center on Privacy and Technology released the Perpetual Line-Up report, which was the result of a year-long investigation and over 100 records requests to police departments around the country. It is recognized as the most comprehensive survey to date of law enforcement use of facial recognition and the risks that it poses to privacy, civil liberties, and civil rights.[xiv] In that report, of the 52 agencies that they found to use (or have used) facial recognition, the Ohio Bureau of Criminal Investigation was the only one whose facial recognition use policy expressly prohibits its officers from using facial recognition to track individuals engaging in political, religious, or other protected free speech activities.

Recommendation #6

The Attorney General should promulgate a specific standard for when law enforcement may utilize facial recognition and define investigative purpose for its use. This standard should require reasonable suspicion that the person to be identified has committed a crime, the person's actions present a danger to human life or may cause serious physical harm, or that law enforcement must use facial recognition to identify someone who is not able to identify him or herself.

The Task Force recommends that rules and regulations are promulgated for facial recognition. As previously mentioned, facial recognition technology is rapidly advancing, its use in Ohio is currently centralized and a new system will be operational in 2021, all of which contribute to the need for more robust, subject matter specific rules and regulations. To support its recommendation, the Task Force presents, in Appendix A, recommended language to govern when law enforcement may utilize facial recognition.

Notably, the Task Force suggests that law enforcement be authorized to utilize facial recognition only where law enforcement has a reasonable suspicion that the particular person(s) to be identified has committed a criminal offense, a reasonable belief that the person's actions present a danger to human life or may cause serious physical harm, or that law enforcement must use facial recognition to identify someone who is not able to identify him or herself.

D. Technology and Images

Recommendation #7

The Attorney General should follow the recommended guidance from the Facial Identification Scientific Working Group (FISWG) for security and maintenance of the system.

The Facial Identification Scientific Working Group (FISWG) per their website[xv] is a group whose purpose is to develop consensus standards, guidelines and best practices for the discipline of image-based comparisons of human features, primarily face, as well as to provide recommendations for research and development activities necessary to advance the state of the science in this field. The Task Force agreed that relying on guidance from FISWG is appropriate in maintaining proper system security and maintenance.

Recommendation #8

The Attorney General should follow the recommended guidance from the National Institute of Standards and Technology (NIST)[xvi] to conduct accuracy assessments of the selected Facial Recognition system.

On December 19, 2019, NIST released a report on a study that evaluated effects of race, age and sex on facial recognition software.[xvii] According to NIST, the results are intended to inform policymakers and to help software developers better understand the performance of their algorithms. Face recognition technology has inspired public debate in part because of the need to understand the effect of demographics on face recognition algorithms.

NIST recommends that facial recognition technology vendors improve their algorithms to achieve no gap in demographics. The December report emphasizes that NIST's testing gives a general sense for an algorithm's accuracy but the actual performance of any individual system will vary depending on how it's set up and the data it uses. For that reason, NIST recommends that programs consider conducting their own accuracy assessments of how their system actually works.

The Task Force learned that NEC, the vendor selected for the new system, is among the top scorers for industry standards. The Task Force suggests the contract with NEC be reviewed to ensure that the accuracy assessments and algorithm adjustments are performed and the system updated as recommended. Further, the Task Force recommends that the author of the NIST report be invited to meet with the OHLEG Steering Committee and the proposed Facial Recognition Advisory Committee.

Recommendation #9

The facial recognition database system should adopt a reasonable image quality standard and disqualify images that do not meet that standard.

Just like with any data system, the performance of a facial recognition system depends on the quality of the image. Image quality is dependent on several factors including background, lighting, angle, facial expression and pose. Poor quality images hinder the performance and compromise the integrity of the facial recognition system and should not be used for an investigative search. Ohio should adopt a reasonable standard for the quality of images that will be enrolled in the database and a reasonable standard for the quality required for probe images. FISWG has issued and regularly updates a set of image quality standards that Ohio should consider adopting.

Recommendation #10
Probe images used by law enforcement should not be enrolled in the facial recognition database.

A probe image, according to the National Sheriffs' Association[xviii], is any unknown image captured for facial recognition. Probe images can be taken by an officer in the field using a camera or mobile phone or from other sources such as security and CCTV cameras. These images can and will vary in quality and consistent with Recommendation #9 should not be enrolled or uploaded into the facial recognition database.

Recommendation #11
The Attorney General should seek agreement from the Department of Public Safety and Bureau of Motor Vehicles (BMV) to enroll current BMV images that meet the requisite image quality standard in the facial recognition database.

The Task Force had several spirited conversations about this issue and, after careful consideration, generally agreed that new images from the BMV should be enrolled in the facial recognition database for purposes of investigation. However, as the discussion concluded Senator Eklund cautioned the group, expressed his dissent and said enrolling the BMV images is not a recommendation he would make or support. The Task Force considered people's privacy interests, public safety and its other recommendations – i.e. a centralized process, mandated training, enhanced audit and monitoring procedures, increased transparency and public education – to tip the scale for enrollment. The frequency of images being imported is subject to agreement between the Attorney General and Department of Public Safety and consequently, the Task Force makes no recommendation.

E. Auditing, Monitoring, Compliance and Transparency

Recommendation #12
Ohio's Facial Recognition Policy should require routine monitoring, periodic audits, enforcement, and public transparency.

The Task Force recommendation is broad; however Appendix B Proposal on Monitoring, Auditing, Enforcement and Transparency provides detail for consideration in future promulgation of Facial Recognition Policy for Ohio. The proposal details the critical topics of data quality assurance, record retention and destruction, accountability and enforcement and search log and audits. A policy that successfully integrated each of these elements would reflect best practices and could serve as a model for other states and localities.

As noted, policy controls that govern agency activity generally contain at least two components: (1) a substantive policy; and (2) a governance structure for ensuring implementation of and compliance with that policy. Effective controls require both. Appendix B focuses on the second component, the governance structure. Specifically, it addresses routine monitoring, annual audits, enforcement and public transparency. Established facial recognition policies, including those that the Task Force has looked to as models (Indiana[xix], Michigan[xx] and the Department of Justice, Bureau of Justice Assistance[xxi]), recognize the importance of establishing such a governance structure.

Some of the recommendations outlined in Appendix B are:

- Ohio should have a policy that sets out how it will monitor, audit and enforce compliance with its facial recognition policies.
- Ohio should have a policy on how it will ensure public transparency with respect to criminal justice agency use of facial recognition.
- The Ohio Facial Recognition System should subject itself to periodic, random compliance and quality audits.
- Individual facial recognition requests and searches should be logged.
- Ohio should be open with the public with regard to face recognition information collection, receipt, access, use, dissemination, retention, and purging practices.
- A state-level office or official should be responsible for enforcement of Ohio's facial recognition policies.
- Ohio should produce an annual report on its use of facial recognition technology for criminal justice purposes and should share this report with the public.

To further inform the Task Force's consideration of monitoring, auditing, enforcement and transparency policies, Ohio State Moritz College of Law's Program on Data and Governance reviewed federal guidelines for how states that utilize facial recognition can address privacy, civil rights, and civil liberties implications, as well as two of the most developed existing state policies (Indiana and Michigan). Appendix C is the memo summarizing these federal and state guidelines and policies. It suggests how Ohio can build on these models.

As noted in Appendix C, to be fully cognizant of potential privacy issues and design a policy that addresses those issues from a forward-looking perspective, Ohio policies should mirror the federal policy template. Notably, federal auditing guidance mentions the use of third-party neutral auditors in order to mitigate internal auditing inherent biases. In order to ensure a more robust and meaningful auditing process, Ohio can involve third-party neutral auditing mechanisms.

Further, Indiana and Michigan currently have strict restrictions on divulgence of any data regarding facial recognition programs. Although these concerns are laudable given the need for protection of personally identifiable information ("PII"), it is recommended that general statistics about complaints, audit results, and policy changes, which do not contain PII, be made available to the public to ensure greater transparency. This would result in accomplishing a higher level of transparency, a goal that federal guidance makes clear is of importance.

F. Public Education

Recommendation #13
The Attorney General should ensure the public has access to information about the use and regulation of facial recognition in Ohio.

The Task Force understands the value of public education and the importance of finding ways to ensure the public has factual information about the use and regulation of facial recognition technology. In addition to the transparency suggestions included in Appendix B and Appendix C pursuant to Recommendation #13 and beyond posting rules, policy and regulations on a dedicated website for facial recognition, there should be features like Frequently Asked Questions (FAQ) to dispel myths and misunderstanding. Additional resources for public consumption may include a list of terminology and definitions, notice that BMV images may be enrolled in the database and case profiles (generally) on how and in what situations the technology is used.

G. Future Discussion

Throughout the Task Force discussions there were several topics proposed but not directly addressed. Those topics are opportunity for further examination and consideration in the evolution of the use of facial recognition technology in Ohio. The topics include:

- Brady implications, if any, relating to the use of facial recognition technology;
- Enrolling images from non-governmental databases (like social media or other publicly available sources);
- The Fourth Amendment implications, if any, of using facial recognition technology; and,
- How or if to offer policy recommendations/guidance to local law enforcement if they use facial recognition technology.

CONCLUSION

The Task Force sincerely thanks Attorney General Yost for his forward-thinking approach to the use of facial recognition technology in Ohio. The Task Force appreciates the opportunity to engage early in a long term, consequential conversation in the evolution of facial recognition as an investigative tool for Ohio law enforcement. This is a pivotal time to consider structure and protocols to build public trust and confidence in powerful technology that has limitations and can be easily misunderstood. It is our intent that the recommendations of the Task Force balance people's privacy interests with the need for public safety while providing scrutiny and increased oversight.

Appendix A

OHIO CURRENT (effective 02-22-17):

http://files.ohleg.org/general/OHLEG_Rules_Regulations.pdf

Facial recognition technology is an investigative tool. Law enforcement should use it to generate an investigative lead in an active criminal matter in order to solve or prevent crime, to reduce an imminent threat to health or safety, or to identify someone who is not able to identify himself or herself. Law enforcement may not employ this technology to conduct dragnet screening of individuals, nor should it use it to facilitate mass surveillance of places, groups, or activities unless doing so furthers an official law enforcement activity. For example, it would not be appropriate for law enforcement to use facial recognition technology to conduct surveillance of persons or groups based solely on their religious, political, or other ~~18~~ constitutionally protected activities or affiliations unless doing so furthers an official law enforcement activity.

Promulgate specific rules, regulations for Facial Recognition to replace 1.11 – 1, 2, 3, 5, 6, 7, 8 to reflect centralized process and other recommendations (audit, compliance, transparency)

The use of the Facial Recognition attribute as an investigative tool will fall under the same rules as those applied to OHLEG CJI with the addition of the following:

1. All Ohio drivers' licenses, ID photos, and all other photos will remain in the custody and control of the originating agency or OHLEG but will not be otherwise transferred to any other entity.
2. Images received in a request or submission will not be stored as enrolled images within the Facial Recognition system. A thumbnail photo will be archived for audit purposes, but the photo will not be enrolled in the database and will not be searchable.
3. Images enrolled in the Facial Recognition system will not be released to anyone other than law enforcement personnel and only in conjunction with an authorized criminal investigation.
4. Facial Recognition technology may only be used for an official law enforcement activity. For the purposes of this section, an "official law enforcement activity" shall mean an activity, carried out by duly authorized law enforcement personnel pursuant to their official duties, that is consistent with law and ~~is grounded in a reasonable belief based on a totality of circumstances that the use of facial recognition may: a. Result in an investigative lead with respect to a specific criminal matter; b. Reduce an imminent threat to health or safety~~; is taken:

(a) pursuant to a reasonable suspicion that the particular suspect(s) to be identified has committed:

1. A felony offense
2. An offense of violence as defined in section 2901.01 (A)(9) of the Ohio Revised Code;

(Examples of these include offense such as Murder, Manslaughter, Rape, Aggravated Menacing, Menacing by Stalking, Abduction, Extorsion, Riot, Escape, Inducing Panic, Domestic Violence, Intimidation.)

3. A sex crime involving juvenile victims;
4. The crime of Criminal Child Enticement; or

(b) pursuant to a reasonable belief that the suspect's continued or imminent actions present a danger to human life or may cause serious physical harm; or

(c) in order to assist in the identification of someone (e.g. a child, or an unconscious or deceased person) who is not able to identify him or herself.

5. Agencies must keep a log with an entry, showing the date of search request, name, case number, and the type of criminal investigation being conducted, for every use of the Facial Recognition attribute.
6. All Facial Recognition requests and any results of the inquiry will be maintained by OHLEG in accordance with appropriate current OHLEG document maintenance and destruction policies.
7. An agency supervisor must approve any dissemination of Facial Recognition images or search results beyond the originating agency.
8. Disseminations to the press will occur only with OHLEG management and requesting agency authorization.

Appendix B

Ohio Attorney General Facial Recognition Task Force
Proposal on Monitoring, Auditing, Enforcement and Transparency

Prepared by
Dennis Hirsch, The Ohio State University Moritz College of Law and Capital University Law School
Brian Ray, Cleveland-Marshall College of Law

January 6, 2020

Overview

Policy controls that govern agency activity generally contain at least two components: (1) a substantive policy; and (2) a governance structure for ensuring implementation of and compliance with that policy. Effective controls require both. This proposal focuses on the second component, the governance structure. Specifically, it addresses routine monitoring, annual audits, enforcement of the AG's policies that govern the facial recognition system, and public transparency. Established facial recognition policies, including those that the Task Force has looked to as models, recognize the importance of establishing such a governance structure. For example, the Indiana Intelligence Fusion Center Face Recognition Policy (June 1, 2019), affirms that the Center "will follow procedures and practices by which it can ensure and evaluate the compliance of users with the face recognition system requirements and with the provisions of this policy and applicable law."[1] Similarly, the US Department of Justice's Face Recognition Policy Development Template states that:

> *The implementation of proven policies and practices can mitigate the risk of negative impacts while improving mission effectiveness. As face recognition use expands, it is necessary for law enforcement, fusion centers, and other public safety agencies to ensure that comprehensive policies are developed, adopted, and implemented in order to guide the entity and its personnel in the day-to-day access and use of face recognition technology. Policies that are developed in a transparent manner and which are properly enforced foster trust—not only within and between justice partners but also by the public. This process helps ensure that justice entities are serving as responsible stewards of face recognition information.*[2]

We have reviewed existing federal and state policy templates documents in order to identify and integrate best practices. Based on this review, we believe that Ohio's Facial Recognition Policy should address routine monitoring, periodic audits, enforcement, and public transparency. A policy that successfully integrated each of these elements would reflect best practices and could serve as a model for other states and localities.

[1] https://www.in.gov/iifc/files/Indiana_Intelligence_Fusion_Center_Face_Recognition_Policy.pdf
[2] https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf

Governance and Transparency Policy Framework

- The Attorney General should have a policy that sets out how it will monitor, audit and enforce compliance with the AG's policies governing the state's use of facial recognition.[3]
- The Attorney General should have a policy on how it will ensure public transparency with respect to the state's use of facial recognition.

Monitoring

- All access to, and use of, facial recognition technology should be logged.[4]
    - The log should record information such as:
        - name and ID of the law enforcement user making the request,
        - identity of the agency requesting facial recognition,
        - name and ID of the trained facial recognition examiner conducting the search,
        - date and time of access to the system,
        - purpose and justification for the search, including the factual basis for a finding of reasonable suspicion of the particular individual to be identified, and a case/complaint number and file class/crime type, if available, and
        - assigned image identification number and date of image capture to uniquely identify the images transmitted in response to the facial recognition query or a notation that no facial images were available.
    - The Facial Identification Scientific Working Group (FISWG) provides a more detailed recommendation as to the type of information to be logged routinely. The AG's Office should consider the FISWG recommendations.
    - The logs should be set up so as to be susceptible to audit.

- The Attorney General should routinely collect and store, on a system-wide basis and subject to the agency's retention policy, information on:
    - the number of facial recognition requests fulfilled;
    - the criminal violation(s) that were associated with each case identifier;
    - the results of each facial recognition request;
    - the results of the investigation(s), if any, associated with each facial recognition request;
    - the disposition of the probe photo in each request, that: (1) fails to produce an investigative lead, (2) does not result in a criminal charge, or (3) results in an acquittal; and,
    - the demographic information for each probe photo evaluated, if known, including sex, age, and race or country of birth.[5]

---

[3] *See, e.g.,* IIFC Face Recognition Policy at 12. ("The IIFC will follow procedures and practices by which it can ensure and evaluate the compliance of users with the face recognition system requirements and with the provisions of this policy and applicable law. This will include logging access to face recognition information, may include any type of medium or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related activity, and will entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least annually, and a record of the audits will be maintained by the Privacy Officer, of the IIFC pursuant to the retention policy. Audits may be completed by an independent third party or a designated representative of the IIFC.")

[4] San Diego Facial Recognition Policy at 9. https://info.publicintelligence.net/CA-SanDiegoFacialRecognitionPolicy.pdf

[5] Patrick Grother, et al., NISTIR 8280: Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (2019), 1.

- The Attorney General designate a person or office to be responsible for monitoring the performance of, and compliance with the policies governing, the state's facial recognition system.[6]
- Routine monitoring of the Ohio facial recognition system should include:[7]
    - ensuring compliance with applicable laws, regulations, standards, and policy,
    - ensuring that access controls are in place and are followed,
    - reviewing face recognition search requests,
    - reviewing the results of face recognition searches and the communication of candidate names or images, if any, to the requesting agency,
    - ensuring that all protocols, including retention and purging protocols, are followed,
    - conducting random evaluations of compliance with system requirements, applicable facial recognition policy and law, with documentation of results, and
    - ensuring and documenting that personnel, including investigators from external agencies who may make face recognition search requests, meet all prerequisites stated in this policy prior to being authorized to access the face recognition system
    - periodic review of the technology with the vendor, identifying potential enhancements to the system;
- There should be a mechanism for system personnel, and those submitting requests to the system, to report errors, malfunctions, or deficiencies of face recognition information or systems, and suspected or confirmed violations of face recognition policies.[8]
- The Attorney General should require law enforcement agencies and individuals that submit requests to or otherwise utilize the system to comply with the AG's policies governing the system. The Attorney General should sanction appropriately those agencies and individuals that do not comply with these policies, including by suspending their ability to submit further requests to or otherwise utilize the facial recognition system.

Auditing

- The Ohio Facial Recognition System should be subject to random, annual compliance and quality audits.[9]
- A responsible official who is sufficiently independent of the Attorney General's Office to enhance the public's confidence in the operation of the system should perform the audit.
- The audit should assess the system for items that include:
    - authorized versus unauthorized use,
    - appropriate justification for system requests, access and use[10],
    - compliance with the standard for when it is appropriate to query the system,
    - performance of trained human reviewers,
    - system accuracy, and
    - Harmful bias on the basis of race, gender, religion, national origin or other protected class status.
- The audit should result in an audit report that should be made available to the public.
- The responsible official should keep a record of all audits and audit reports, subject to the agency's retention policy.

[6] US DOJ Facial Recognition Policy Template at 16.
[7] Id.
[8] *Id.* at 34.
[9] Id.
[10] *See, e.g., Id.* Section VIII: "All FR use is subject to audit by the MSP SNAP Unit. In the event of an audit, the User will be required to provide appropriate justification for the use of FR."

- As part of the periodic audit, Ohio should benchmark its facial recognition technology practices and policies against those of other federal, state and local agencies and the latest advances in the field. The audit should recommend any relevant updates to ensure that Ohio's facial recognition technologies, practices and policies remain up to date.[11]

Enforcement

- The Attorney general should designate a state-level office or official to be responsible for the AG's policies governing the facial recognition system.
- If an agency, or agency personnel, are found to be in violation of Attorney General's policies governing the facial recognition system, this should result in an appropriate sanction up to and including suspension of the agency's or person's ability to query or otherwise utilize the facial recognition system and referral of the matter to appropriate authorities for potential criminal prosecution where necessary to effectuate the purposes of the facial recognition policy.[12]

Transparency

- Ohio should be open with the public with regard to face recognition information collection, receipt, access, use, dissemination, retention, and purging practices.[13]
- The Attorney General's policies governing the facial recognition system should themselves be publicly available.
- The Attorney General should inform the public about the structure of the facial recognition system, including descriptions of:
    - facial recognition technology or platform the State is using, including contracted providers, systems, and database,
    - Databases searched and sources of the images within each such database."
    - who can access the system, including its databases of images,
    - who can perform match queries in the system,
    - who can download, access, or use images imported into the system's databases outside of the system, i.e. who, if anyone, has access to imported images for secondary purposes, and
    - the standards sand policies that govern the facial recognition system.
- The Attorney General should quarterly disclose to the public system information including:
    - the number of facial recognition requests made within each quarter,
    - the number of facial recognition requests fulfilled within each quarter,
    - the agencies or offices making these requests,
    - the purposes of these requests,
    - the criminal violation(s) that were associated with each case identifier,
    - the databases searched,
    - the results of the facial recognition requests, and
    - the results of the investigation(s), if any, associated with facial recognition requests.
- The Attorney General should make publicly available each audit of the facial recognition system.[14]
- The Attorney General should produce an annual report on the state's use of facial recognition technology for criminal justice purposes and should share this report with the public.

---

[11] *See, e.g.,* Indiana Intelligence Fusion Center at 12: "The Assistant Director, will review and update the provisions contained in this face recognition policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the face recognition system; the audit review; and public expectations."

[12] See, e.g., Id. at

[13] *See,* US DOJ Facial Recognition Policy Template at 33.

[14] *Id.* at 34.

Memorandum

Moritz College of Law
280A-1 Drinko Hall
55 W. 12th Ave.
Columbus, OH 43210

Appendix C

January 13, 2020

Ohio Attorney General Facial Recognition Task Force
Proposal on Monitoring, Auditing, Enforcement and Transparency

Prepared By
Dennis Hirsch, The Ohio State University Moritz College of Law
Angad Chopra, Research Assistant for the Program on Data and Governance

To further inform the Task Force's consideration of monitoring, auditing, enforcement and transparency policies, Ohio State Moritz College of Law's Program on Data and Governance reviewed federal guidelines for how states that utilize facial recognition can address privacy, civil rights, and civil liberties implications, as well as two of the most developed existing state policies (Indiana and Michigan). This memo summarizes these federal and state guidelines and policies. It suggests how Ohio can build on these models.

Federal Level Model Face Recognition Policy Considerations

At the federal level, the United States Departments of Justice ("DOJ") and Homeland Security ("DHS") have provided guidance on the implementation of facial recognition policies in the United States. In particular, the DOJ created a template for State, Local, and Tribunal Criminal Intelligence and Investigative Activities. The template's suggestions are designed to inform best practices, in an attempt to mitigate, as much as reasonably possible, risks stemming from privacy, civil rights, and civil liberties ("P/CRCL").[15] This DOJ template provides a model policy which State and Local authorities can use as a starting point in the development of facial recognition procedures in the context of criminal investigation. This federal guidance synthesizes information garnered from multiple federal agencies regarding monitoring, auditing, enforcement, and transparency and then provides a model policy for newly developed facial recognition system. Relying on information gleaned from commercial/private-sector implementation as well as various studies involving facial recognition technology, the DOJ was able to identify risks involving privacy, P/CRCL. As federal guidance provides a robust approach to face recognition policies, while carefully noting potential P/CRCL problems, Ohio should mirror the federal policy template as closely as possible, so as to be fully cognizant of potential privacy issues and design a policy that addresses these problems from a forward-looking perspective.

Monitoring

Federal guidance suggests that state and local authorities implementing facial recognition processes in the context of criminal investigation should ensure continuous monitoring which comprises of "ongoing

[15] *See* https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf; https://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component [*hereinafter DOJ Face Recognition Policy Template*]

situational awareness of information security, vulnerabilities, threats, and incidents for each user level to support entity risk management decisions."[16] Specified in DOJ federal guidance are high level monitoring stages and on-the-ground monitoring processes.

- High-level Monitoring Stages:
    1. Educate and raise awareness of the importance of having P/CRCL protections with participating criminal investigatory agencies.
    2. Assess entity P/CRCL risks by evaluating the process through which the entity collects, receives, accesses, uses, disseminates, retains, and purges face recognition information
    3. Develop a face recognition policy to articulate the legal framework and policy position on how the entity faces recognition
    4. Perform a policy evaluation and engage with community stakeholders, prior to publishing, to determine whether the policy adequately addresses current standards, P/CRCL protections, and the law.
    5. Implement and train personnel and authorized users on the established rules and procedures
    6. Perform an annual policy review and make appropriate changes in response to implementation experience, guidance from oversight or advisory bodies, applicable laws, technology, and public expectations.[17]
- On-the-ground monitoring procedures
    1. Identify a clear purpose in a written "statement of purpose" clearly articulating policies for established authorized use, limitations on access, and use of recognition systems.[18] Additionally, identify the level of training required of officers who use such systems.[19]
    2. Clearly identify what information is subject to face recognition policies, who is subject to face recognition policies and how the entity's face recognition policy is made available to personnel.[20] Additionally ensure that all personnel and information-originating and user agencies are in compliance with all applicable constitutional and statutory laws.[21]
    3. Clearly establish a chain of command delineating who has the primary responsibility for the entity's overall operation, including justice information systems, face recognition program and system, information collection and retention procedures, coordination of personnel, and enforcement of this policy.[22] Ensure higher levels on the chain-of-command have appropriate disciplining and accountability mechanisms in place, ensuring all protocols are followed as delineated in the policy.[23]
    4. Provide information about the designated and trained privacy officer who will handle reported errors and violations of the policy and who will oversee the implementation of the policy, specifically monitoring P/CRCL considerations.[24]

Auditing

At the federal level, the DOJ has recognized the importance of implementing auditing procedures after the establishment of a new face recognition policy. Importantly, the DOJ notes the following procedures to ensure an adequate audit mechanism:

- Establish oversight officers who are constantly reviewing complaints and the overall policy

[16] *Id.* at 41.
[17] *Id.* at 2.
[18] *Id.* at 13-14.
[19] *Id.* at 14.
[20] *Id.* at 15
[21] *Id.* at 16
[22] *Id.* at 16.
[23] *Id.*
[24] *Id.* at 17-18

scheme for any P/CRCL concerns. Conduct an annual review of the policy in response to changes in law and program implementation experience. *If possible, auditing responsibilities should be transferred to third-party neutral organizations that are not involved with governmental or regulatory investigation.*

- Establish a random, periodic audit and evaluation schemes to ensure user compliance with system requirements.
- Confirm through random audits that face recognition information is purged in accordance with the policy.[25]
- For any instance of noncompliance with the policy or other issue discovered under an audit, identify the underlying reason (i.e. training issue, policy gap, technology issue, deliberate misuse).[26]

Enforcement

- Clearly identify and establish a state-level, participating agency tasked with enforcing the provisions of the established face recognition policy.
- Establish levels of discipline for noncompliance with the policy determined by continual monitoring and auditing. Disciplinary measures can include: suspension, discontinuation of access to information, and criminal prosecution.[27]

Transparency

- Ensure that those participating in the face recognition policy will be open with the public with regard to face recognition information collection, receipt, access, use, dissemination, and purging practices. Policies should be made available on consumer webpages.[28]
- Establish a point of contract through which the public can receive and respond to inquiries and complaints about participating entity's use of face recognition systems and P/CRCL issues.[29]
- Share results of third-party neutral audits and enforcement proceedings with the public, identifying problematic trends and resolutions to those identified issues on a periodic basis and publish results to an accessible webpage ensuring that the consuming public have access to such results.

State-level Implementation

At the state and local level, jurisdictions have already implemented facial recognition policies in the context of criminal investigation. These policies tend to closely mirror federal guidance, with few omissions or nuances, seemingly as a protective measure to ensure P/CRCL complications are avoided. As of the date of this writing, state implementation policies are fairly nuanced. As such, auditing procedures and potential areas of improvement are, as of yet, not completely understood. Using Indiana and Michigan as state-wide case studies, Indiana has put forward the most robust facial recognition policy, while Michigan's policy is quite a bit more lax than federal guidance would recommend. Still, both states adhere to the core four elements (monitoring, auditing, enforcement, and transparency). To the extent possible, it is recommended that Ohio implement a facial recognition policy that addresses auditing, transparency, and enforcement in a way that more closely resembles federal guidance so as to mitigate P/CRCL issues.

---

[25] *Id.* at 17, 22, 24, 30, 32.

[26] *See* http://it.ojp.gov/GIST/181/Privacy--Civil-Rights--and-Civil-Liberties-Audit-Guidance-for-the-State--Local--Tribal--and-Territorial-Intelligence-Component at 29 [*hereinafter P/CRCL DHS Auditing Handbook*]

[27] *DOJ Face Recognition Policy Template* at 35.

[28] *Id.* at 33.

[29] *Id.*

The following analysis provides details of Indiana and Michigan's face recognition policies and provides insight into how closely the DOJ's federal guidance has been followed by both states. At the end of each section, a "possible areas for enhancement" section is included to identify differences between the state policy and the federal guidance. Recommendations are added as possible measures to enhance a future Ohio face recognition policy in a way that reduces P/CRCL concerns.

Monitoring

- **Indiana**[30]
  - Indiana has crafted a clear purpose statement following DOJ guidance in their model template.[31]
  - Within this purpose statement, Indiana identifies polices for established authorized use, limitations on access, and use of face recognition systems. Levels of training required for participation is also identified. [32]
  - Indiana identifies what information is subject to face recognition policies, who is subject to the policies, and how the policy is made available to personnel. Government oversight has been established to ensure the policy and personnel are adhering to all applicable statutory/regulatory law.[33]
  - Indiana has identified the Indiana Intelligence Fusion Center ("IIFC") as the appropriate oversight body overlooking all policy implementation procedures. The IIFC's Executive Director is responsible for administering the policy's program and ensuring compliance with laws, regulations, standards, and policy[34]

- **Michigan**[35]
  - Michigan's monitoring procedures are not as robust as federal guidance recommends. Still, Michigan tasks the MSP SNAP Unit with official monitoring responsibilities, to ensure that participating agencies comply with all applicable statutory/regulatory provisions.[36]
  - Michigan has a policy that requires that there is a purpose behind facial recognition data accumulation and before an agency attempts to gather such information a purpose must be stated.[37]

Auditing

- **Indiana**
  - Importantly, Indiana's auditing procedures do not conflict with privilege given to law enforcement investigative agencies. Although audits *may* be conducted by a third-party neutral organization, internal audits are also approved. As such, these internal audits would make external review difficult due to the privilege associated with law enforcement agencies. It is recommended that Ohio adopt strategies for third-party neutral audits so that the public is able to view audit reports and results to identify potential P/CRCL

[30] *See* https://www.in.gov/iifc/files/Indiana_Intelligence_Fusion_Center_Face_Recognition_Policy.pdf [*hereinafter Indiana Intelligence Fusion Center Face Recognition Policy*]
[31] *Id.* at 5.
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *See* https://www.michigan.gov/documents/msp/SNAP_Acceptable_Use_Policy_2016_03_07_533938_7.pdf [*hereinafter Michigan SNAP Acceptable Use Policy*].
[36] *Id.* at 4.
[37] *Id.* at 2.

issues.[38]
    - Indiana notes that it will follow procedures and practices to ensure and evaluate compliance of users with its face recognition policy. Indiana has delineated a system of random auditing so as not to establish a discernable pattern that may influence users' actions. These audits will be conducted annually, and record of the audits will be maintained by the IIFC but *must not* be published.[39]
    - IIFC's Assistant Director will review the policy annually and update provisions in order to comply with changes in applicable law, technology, audit results, public expectations, or the purpose of the policy.[40]

- **Michigan**
    - All Michigan facial recognition use will be subject to audit by the MSP SNAP Unit. Audit findings are collected at the sole discretion of the MSP SNAP Unit, as such external review is limited. These audits are randomized and if an entity comes under audit, such entity must provide an appropriate justification for the use of the facial recognition. Once again, audit procedures are restricted far more than federal guidance would suggest.[41]

- **Possible Areas for Enhancement**
    - Federal auditing guidance mentions the use of third-party neutral auditors in order to mitigate internal auditing inherent biases.[42] In order to ensure a more robust and meaningful auditing process, Ohio can involve third-party neutral auditing mechanisms.

Enforcement

- **Indiana**
    - Mirroring federal guidance and in the event of noncompliance with the policy, IIFC personnel can suspend/discontinue access, apply appropriate disciplinary or administrative actions/sanctions, and refer the matter for criminal prosecution.[43]

- **Michigan**
    - The MSP SNAP Unit are given complete discretion to issue penalties that include, but are not limited to, termination of use by an agency and criminal prosecution.[44]

Transparency

- **Indiana**
    - Indiana has limited public disclosure of face recognition information and audits and will only provide information to the public in compliance with IIFC's privacy policy. This approach limits transparency and does not closely mirror the recommendations listed in federal guidance.[45]
    - Indiana's face recognition policy is easily accessible and posted on the Indiana State Government website.

---

[38] *See Indiana Intelligence Fusion Center Face Recognition Policy* at 6.
[39] *Id.* at 12.
[40] *Id.*
[41] *See Michigan SNAP Acceptable Use Policy* at 4.
[42] *DOJ Face Recognition Policy Template* at 34.
[43] *See Indiana Intelligence Fusion Center Face Recognition Policy* at 12.
[44] *Michigan SNAP Acceptable Use Policy* at 4.
[45] *See Indiana Intelligence Fusion Center Face Recognition* at 10.

- **Michigan**
  - Michigan classifies all information retained from the SNAP program as highly confidential personal identifiable information, which can only be disclosed in accordance with federal laws.[46]
  - Michigan does not delineate publication of audit results or any other reviewing proceedings. The policy, however, is easily accessible on the Michigan State government website.[47]

- **Possible Areas for Enhancement**
  - Indiana and Michigan currently have strict restrictions on divulgence of any data regarding face recognition programs. Although these concerns are laudable given the need for protection of personally identifiable information ("PII"), it is recommended that general statistics about complaints, audit results, and policy changes are made available to the public to ensure greater transparency. This would result in accomplishing a higher level of transparency, a goal that federal guidance makes clear is of importance.

[46] *Michigan SNAP Acceptable Use Policy* at 2.
[47] *See generally id*.

Appendix D

Office of the Ohio Public Defender

Timothy Young, State Public Defender

Memorandum on Ohio's Use of Facial Recognition Software

There are serious questions about the error rate associated with facial recognition technology. This is compounded by serious privacy and Constitutional concerns under a regulatory system for facial recognition technology that includes no legislative guidance or judicial check on its use. As a result, the initial question this working group should assess is not whether the technology should be centralized or diffuse. It is whether the technology should be used at all.

Scientifically reliable forensic technology can aid law enforcement in efforts to solve crime, exonerate the innocent, and protect public safety. Perhaps the most powerful example of this is the emergence of DNA analysis.1 But subjective feature comparison techniques, when not scientifically validated, can lead to wrongful arrests and convictions.2 At its core, facial recognition is a feature comparison method that is comparable to microscopic hair analysis, latent fingerprint analysis, and firearm analysis.3 Because we lack sufficient evidence to demonstrate that the error rate associated with facial image comparison is within an acceptable range, we do not currently know if use of this technology will add to the reliability of law enforcement investigations (like non-mixture DNA analysis might) or result in wrongful convictions (as in the case of microscopic hair analysis).

I. Human and Technological Error Rates.

It has been repeatedly emphasized in this working group that low quality probe images will result in low quality lists of potential candidates. Consequently, human discretion—trying to compare a probe image to a list of 10 to 20 other images—will play a considerable role in turning algorithmic output into a useable investigative lead. There is significant reason for concern with both the rate of technology error and the rate of human error in a facial recognition process. These error rates are significant in both their size and import: they can result in the arrest and prosecution of innocent people.

When facial recognition technology is combined with the false cultural belief that this type of "CSI" science is infallible, not only is there a risk that innocent people will be convicted, it is certain. "Although witnesses can often be very confident that their memory is accurate when identifying a suspect, the malleable

nature of human memory and visual perception makes eyewitness testimony one of the most unreliable forms of evidence."[4] Despite the well-intentioned and sincere statements of the prosecutors on the working group that this new technology will only be used as an investigative tool, it will only be a short time before prosecutors who are not members of this working group seek to introduce the technology as evidence of an identification. The stakes here are high: "[m]istaken eyewitness identifications contributed to approximately 71% of the more than 360 wrongful convictions in the United States overturned by post-conviction DNA evidence."[5]

That it will be offered in criminal cases is a given, not a question. Prosecutors may seek to avoid Confrontation Clause objections by having an analyst who uses the software testify.[6] And the current acknowledged issues with reliability will not stop proponents from arguing that the technology should be assessed by factfinders. Today, bite mark evidence is still offered and admitted in courts across this country, including Ohio. This is despite the fact that is beyond debunked.[7] "[B]itemark analysis does not meet the scientific standards for foundational validity, and is far from meeting such standards. To the contrary, available scientific evidence strongly suggests that examiners cannot consistently agree on whether an injury is a human bitemark and cannot identify the source of [a] bitemark with reasonable accuracy."[8] Hair analysis is a perfect example of a technology falsely considered to be reliable based upon the social belief in the infallibility of forensic science. Not only did juries believe hair comparisons because it was dressed up in scientific regalia, those who did the analysis also became enamored of its false promises and claimed scientific certainty where there was no science at all – just microscopic pattern matching.

A. Technological Error.

The first source of error is the database of pictures against which a probe photo is compared. The database does not include the full population of people who could conceivably commit a crime in Ohio.[9] For example, the current database includes BMV photos through 2011.[10] If someone who moved to Ohio after 2012 commits a crime that is caught using surveillance video, running the probe photograph through our current database will not identify the actual perpetrator as a suspect. But updating the database to include all Ohio residents will not solve this problem. If an Ohioan has an out-of-state sibling with similar facial features who commits a crime while visiting Ohio, the database does not include the suspect but at least one person who may be identified as a false positive.

The second source of error comes from algorithmic bias. For example, MIT researchers have found that facial recognition algorithms tend to have higher rates of misidentification for women and people of color.[11] A notable experiment done by the ACLU of Northern California involved running members of Congress through Amazon's

facial recognition software.[12] The software misidentified 28 members of Congress, disproportionately impacting members who are not white men.[13]

B. Human Error.

One potential guardrail to mitigate the risk of technological error is human discretion. But in these circumstances, human discretion runs the risk of exacerbating error risks, not curbing them. Currently, human beings who compare images of unfamiliar faces to determine whether they show the same person get it wrong 20-30% of the time.[14] Multiple training courses exist to help people become better at comparing unfamiliar faces.[15] These training courses have not been empirically validated to assess whether attendance increases proficiency.[16] However, recent evaluations have shown that one-hour and half-day courses have no impact on proficiency and longer courses produce only small and inconsistent improvements.[17]

The evidence is clear that human beings in controlled settings are not skilled at comparing the faces of strangers. In an investigative setting—where analysts may have more information about *why* a facial recognition search is being run— error rates may be exacerbated by cognitive bias.[18] And while the assurance is that only trained professionals will access the results and make the final comparisons, this is exactly the failure that was seen in hair analysis. It still comes down to a person saying, "in my opinion, this looks just like the other." There is no evidence that increased training will increase reliability of identification. But because it is generated by technological means, it looks and feels like it is more reliable. A rich body of literature demonstrates the ways in which humans who are conducting feature comparison may be influenced by additional investigative information (such as whether the person to be identified is a suspect or victim, whether there is additional information of guilt, etc.).[19]

C. Qualified Immunity Impacts Risk Assessment.

Given the significant risk of errors made by machines and humans alike, use of facial recognition software in ways that could result in the loss of liberty or life may result in significant negative consequences for factually innocent people.[20]

When other innovations carry significant risks, private companies that use them face liability. That liability is a significant factor in the adoption of new, untested technology. The litigation over opiates and Boeing's 737-Max are just two examples that demonstrate this axiom.[21]

The doctrine of qualified immunity—which shields government officials from liability—may indirectly shift the risk analysis associated with error rates in facial recognition.[22] Any public company that uses facial recognition technology to identify shoplifters could face enormous liability for false arrest. This fact informs any cost-

benefit analysis to use of private facial recognition technology for security purposes (as opposed to other commercial purposes). And at this level of inquiry—where the policy questions about a technology are being debated—we should look directly at those error rates associated with the technology and resist the urge to filter it through the lens of qualified immunity.

II. Structural and Constitutional Concerns.

Given the potential issues with facial recognition software, legislative scrutiny and judicial review are integral to ensuring that, if it is used at all, it is used in a way that respects civil liberties. But the current proposals for Ohio's facial recognition rollout are regulated only administratively in the executive branch and require no level of individualized suspicion before use.(23)

The current absence of required individualized suspicion before accessing a facial recognition database raises possible Fourth Amendment concerns after the United States Supreme Court's decision in *Carpenter v. United States.(24)* In *Carpenter*, the Court recognized that government access to digital information can create significant privacy concerns because it allows the possibility of "tireless and absolute surveillance."(25) This digital Fourth Amendment jurisprudence reimagines the "reasonable expectation of privacy" that citizens have, giving rise to the possibility that running a probe photograph through facial recognition software is a search.(26) If running facial recognition technology is a search, then an executive regulatory regime that requires no individualized suspicion or judicial review is insufficient to satisfy the Constitution's demands.

III. Other Jurisdictions are Banning Use of Facial Recognition Technology.

Given the forensic and Constitutional concerns with facial recognition technology, it should not come as a surprise that there is a robust debate about whether law enforcement should have access to it. Michigan currently uses a facial recognition regime that is centralized and requires a showing of probable cause before it is used.(27) Despite having one of the most rights protective regimes in the country, Michigan's legislature is currently considering a bill to ban use of the technology entirely.(28) If this bill passes, Michigan will join municipalities like Oakland, CA; San Francisco, CA; and Somerville, MA which have banned the technology.(29)

Conclusion.

The initial question about facial recognition technology—whether we should use it—has not yet been adequately answered. Further debate about the use of facial recognition technology should be happening publicly in the General Assembly, and not simply within the confines of an executive working group. We should consider a recommendation that bans the use of facial recognition technology until the legislature expressly authorizes its use after transparent conversation about its significant social costs.

1 *See* LaPort, "Wrongful Convictions and DNA Exonerations: Understanding the Role of Forensic Science." NIJ Journal 279, April 2018, available at: https://www.ncjrs.gov/pdffiles1/nij/250705.pdf.

2 *See* President's Council of Advisors on Science and Technology (PCAST) Report to the President on Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods (2016) available at: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.

3 *See* Towler et. al, "Do Professional Facial Image Comparison Training Courses Work?" PLoS ONE 14(2) (2019), available at: https://doi.org/10.137/journal.pone.0211037

4 The Nation Center for State Courts, The Trouble with Eyewitness Identification Tesitmony in Criminal Cases, https://www.ncsc.org/microsites/trends/home/Monthly-Trends-Articles/2017/The-Trouble-with-Eyewitness-Identification-Testimony-in-Criminal-Cases.aspx

5 The Innocence Project, Eyewitness Identification Reform, https://www.innocenceproject.org/eyewitness-identification-reform/

6 This technique for introducing algorithmic evidence has already resulted in admission of DNA evidence obtained via probabilistic geneotyping software such as STRMix and TrueAllele. *See State v. Mathis*, 8th Dist. Cuyahoga No. 107365, 2019-Ohio-3654, ¶ 37 ("Scott discussed the testing performed on a swab taken from the interior crotch area of A.T.'s underwear including an analysis that implemented a computer program called "TrueAllele." She explained that "TrueAllele is a computer program that will basically look at the data in the sample, and it will infer geneotypes from that data or profiles from that data.").

7 PCAST Report, Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf, at 83.

8 *Id.*

9 *See* Ohio Attorney General Special Report: Facial Recognition Inquiries (2019) available at: https://www.ohioattorneygeneral.gov/FacialRecognitionInquiriesReport.

10 *Id.*

11 *See* Buolamwini et al, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," Proceedings of Machine Learning Research 81:1-15 (2018) available at: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

12 https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazonsface-recognition-falsely-matched-28

13 *Id.*

14 Towler, supra note 3.

15 *Id.*

16 *Id.*

17 *Id.*

18 PCAST, supra note 2.

19 See, for example: Dror and Hampikian. "Subjectivity and bias in forensic DNA mixture interpretation." Science & Justice, Vol. 51, No. 4 (2011): 204-8; Miller, L.S. "Procedural bias in forensic examinations of human hair." Law and Human Behavior, Vol. 11 (1987): 157; and Bieber, P. "Fire investigation and cognitive bias." Wiley Encyclopedia of Forensic Science, 2014, available through onlinelibrary.wiley.com/doi/10.1002/9780470061589.fsa1119/abstract.

20 *See* Cover, "Violence and the Word," 95 Yale L.J. 1601 (1986) ("Legal interpretation takes place in a field of pain and death.")

21https://www.cnn.com/2019/05/21/politics/boeing-737-max-lawsuit-1990scrashes/index.html; https://www.npr.org/sections/health-shots/2019/10/15/761537367/your-guide-to-themassive-and-massively-complex-opioid-litigation

22 *Kisela v. Hughes*, 584 U. S. ___(2018).

23 Garvie et. al, "The Perpetual Line-Up: Unregulated Police Face Recognition in America," Georgetown Law Center on Privacy and Technology (2016) at Fig. 9 available at: www.perpetuallineup.org

24 138 S.Ct. 2206, 201 L.Ed.2d 507 (2018).

25 *Id.* at 2218.

26 *See* Snyder, "Faceprints and the Fourth Amendment: How the FBI Uses Facial Recognition Technology to Conduct Unlawful Searches," 68 Syracuse L.Rev. 255 (2018).

27 *See* Garvie, supra note 23.

28 https://www.metrotimes.com/news-hits/archives/2019/07/11/house-bill-would-banfacial-recognition-technology-in-michigan

29 https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html

Appendix E

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

October 25, 2019
The Honorable Sara Andrews, Chair
Attorney General Yost's Facial Recognition Task Force
30 E. Broad Street, 17th Floor
Columbus, Ohio 43215

RE: Ohio Facial Recognition Taskforce

Dear Chair Andrews and Members of the Task Force:

I am writing on behalf of Microsoft to applaud the creation of the Facial Recognition Taskforce in Ohio. At Microsoft, we fundamentally believe in the power of advancing technology to bring important and exciting societal benefits. But we also recognize that as with all tools, technology also brings the potential for abuse. In our view, as technology companies create new and innovative technologies that are rapidly changing the world, they also have an obligation to help address the challenges and concerns that such changes bring. For these reasons, we support the Taskforce's work to study the potential benefits and impacts of the use and development of facial recognition technology, which generally refers to the ability of a computer to recognize people's faces from a photo or through a camera.

We are also calling upon governments to start adopting laws to regulate facial recognition technology. For while this technology is providing and promises to provide tremendous benefits to people, businesses, and governments, it also raises serious issues that go to the heart of fundamental human rights like privacy and freedom of expression. These issues heighten responsibility for tech companies that create these products, and they also call for thoughtful government regulation that balances, among other things, the need for public safety with the essence of our civil liberties.

I. Ongoing developments regarding facial recognition technology

Facial recognition technology has been advancing rapidly over the past decade, and it is being used more and more by each and every one of us in our daily lives. If you have ever tagged a face with a suggested name on a social media platform, used Windows Hello to access your Surface device, or used automated software to catalogue your electronic photos, you have used facial recognition technology.

So, what is changing now? Among other things, computer vision has gotten much better and much faster at recognizing people's faces. This advancement is due to a number of things. It stems from the

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

development of better cameras, sensors and machine learning capabilities. It reflects the advent of larger and larger datasets as more images of people are stored online. It also reflects the ability to use the cloud to connect all this data and facial recognition technology with live cameras that capture images of people's faces and seek to identify them – in more places and in real time.

As facial recognition technology continues to spread, as its use continues to grow, it is empowering real people to accomplish things that they could not have accomplished before. For example, police in New Delhi recently trialed facial recognition technology and identified almost 3,000 missing children in four days.[48] Historians in the United States have used the technology to identify the portraits of unknown soldiers in Civil War photographs taken in the 1860s.[49] Researchers have successfully used facial recognition software to diagnose a rare, genetic disease in Africans, Asians and Latin Americans.[50] And in October of last year, the National Australia Bank designed a proof of concept to enable customers to withdraw money more securely from an Automatic Teller Machine using facial recognition and a PIN.[51]

II. Concerns about bias and discrimination

However, the use of facial recognition technology has also give rise to serious concerns. Biases have been found in the performance of several fielded face recognition technologies. The technologies worked more accurately for white men than for white women and were more accurate in identifying persons with lighter complexions than people of color. While researchers across the tech sector are working overtime to address these challenges, and although significant progress is being made, as important research has demonstrated, deficiencies remain.[52]

Even if biases are addressed and facial recognition systems operate in a manner deemed fair for all people, we will still face challenges with potential failures. Facial recognition, like many AI technologies, typically have some rate of error even when they operate in an unbiased way. And the issues relating to facial recognition go well beyond questions of bias themselves, raising critical questions about our fundamental freedoms.

[48] See https://timesofindia.indiatimes.com/city/delhi/delhi-facial-recognition-system-helps-trace-3000-missing-children-in-4-days/articleshow/63870129.cms.
[49] See https://www.civilwarphotosleuth.com/.
[50] See https://www.genome.gov/news/news-release/Facial-recognition-software-helps-diagnose-rare-genetic-disease.
[51] See https://news.microsoft.com/en-au/2018/10/23/nab-and-microsoft-leverage-ai-technology-to-build-card-less-atm-concept/.
[52] See http://gendershades.org/.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

III. Problems that need to be addressed

We need to be clear-eyed about the risks and potential for abuse regarding the development and use of facial recognition technology. In fact, we believe there are at least three problems that governments need to address. First, especially in its current state of development, certain uses of facial recognition technology increase the risk of decisions and, more generally, outcomes that are biased and, in some cases, in violation of laws prohibiting discrimination. *Second,* the widespread use of facial recognition technology can lead to new intrusions into people's privacy. *And third*, the use of facial recognition technology by a government for mass surveillance threatens to chill democratic freedoms.

We believe that all three of these problems should be addressed through legislation.

IV. Addressing bias and discrimination

In the current state of its development, certain uses of facial recognition technology increase the risk of decisions, outcomes and experiences that are biased and potentially in violation of discrimination laws. Recent research has demonstrated, for example, that some facial recognition technologies have encountered higher error rates when seeking to determine the gender of women and people of color. This makes it especially important that Microsoft and other tech companies continue the work needed to identify and reduce these errors and improve the accuracy and quality of facial recognition tools and services. This work is underway, and we're making important progress. It's equally critical that we work with customers closely to ensure that facial recognition services are deployed properly in ways that will reduce these risks. Over time, we believe that well-functioning market forces can encourage the technology innovation that is needed.

But we also believe that new laws are needed in this area, and for two distinct reasons. First, market forces will work well only if potential customers are well-informed and able to test facial recognition technology for accuracy and risks of unfair bias, including biases that arise in the context of specific applications and environments. Tech companies currently vary in their willingness to make their technology available for this purpose. As a result, some academic tests of these services have omitted some of the market leaders. And when important advocacy organizations have tried to perform tests, they've almost immediately been met by rejections and criticism by some providers who claim that the testing is deficient. As a society, we need legislation that will put impartial testing groups like Consumer Reports and their counterparts in a position where they can test facial recognition services for accuracy and unfair bias in a transparent and even-handed manner.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

V. Protecting people's privacy

The widespread use of facial recognition technology can lead to new intrusions into people's privacy. For example, every public establishment could install cameras connected to the cloud with real-time facial recognition services.

Interestingly, the privacy movement in the United States was born from improvements in camera technology. In 1890, future Supreme Court Justice Louis Brandeis took the first step in advocating for privacy protection when he co-authored an article with colleague Samuel Warren in the Harvard Law Review advocating "the right to be let alone."[53] The two argued that the development of "instantaneous photographs" and their circulation by newspapers for commercial gain had created the need to protect people with a new "right to privacy."

Technology today gives a new meaning to "instantaneous photographs" that Brandeis and Warren probably never imagined. From the moment one steps into a shopping mall, it's possible not only to be photographed but to be *recognized* by a computer wherever one goes. Beyond information collected by a single camera in a single session, longer-term histories can be pieced together over time from multiple cameras at different locations. A mall owner could choose to share this information with every store. Stores could know immediately when you visited them last and what you looked at or purchased, and by sharing this data with other stores, they could predict what you're looking to buy on your current visit.

Our point is not that the law should deprive commercial establishments of facial recognition technology. To the contrary, we are among the companies working to help stores responsibly. But people certainly deserve to know when this type of technology is being used, so they can ask questions and have the opportunity to exercise choice if they wish. Indeed, we believe that this type of transparency and consumer empowerment is vital for building public knowledge and confidence in this technology.

VI. Protecting democratic freedoms and human rights

The use of facial recognition technology by government could raise concerns about encroachments on democratic freedoms and human rights. Democracy has always depended on the ability of people to assemble, to meet and talk with each other and even to discuss their views both in private and in public. This in turn relies on the ability of people to move freely and without constant government surveillance.

There are many governmental uses of facial recognition technology that will protect public safety and promote better services for the public without raising these types of concerns. There is an increasing

[53] See http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

number of such services in place already, and we should encourage them subject to the other protections described here.

But there is one potential use for facial recognition technology that could put our fundamental freedoms at risk. When combined with ubiquitous cameras and massive computing power and storage in the cloud, a government could use facial recognition technology to enable continuous surveillance of specific individuals. It could follow anyone anywhere, or for that matter, everyone everywhere. It could do this at any time or even all the time. This use of facial recognition technology could unleash mass surveillance on an unprecedented scale.

Unprecedented, but not unimagined. As George Orwell described in his novel "1984," one vision of the future would require that citizens must evade government surveillance by finding their way secretly to a blackened room to tap in code with hand signals on each other's arms – because otherwise cameras and microphones will capture and record their faces, voices and every word. Orwell sketched that vision nearly 70 years ago. Today technology makes that type of future possible.

But not inevitable.

We must ensure that the year 2024 doesn't look like a page from the novel "1984." An indispensable democratic principle has always been the tenet that no government is above the law. Today this requires that we ensure that governmental use of facial recognition technology remain subject to the rule of law. It requires ensuring that there will be appropriate public oversight, transparency, and accountability regarding government's use of facial recognition technology. And it requires legislators to consider the standards and circumstances under which court orders should be obtained to authorize government's use of facial recognition technology. To this end, lawmakers can look to the approach taken by the U.S. Supreme Court in *Carpenter v. United States*.[54] *In Carpenter, the Court held* that the government cannot obtain without a search warrant the cellphone records that show the cell sites, and hence the physical locations, where someone has traveled. In, Chief Justice John Roberts wrote for a majority of the court that an individual has a "legitimate expectation of privacy in the record of his physical movements" that are recorded in these cell site records.

Even though we travel with our phones in public and in effect share our location with our cellular provider, the Supreme Court concluded that our location records are covered by the Fourth Amendment to the Constitution and its protection of our right to be secure in our "persons, houses, papers, and

[54] 138 S. Ct. 2206 (2018).

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

effects, against unreasonable searches and seizures." Therefore, the court decided that the government cannot track our movements through our phones and these cell site records unless it secures from an independent judge a search warrant based on probable cause to believe that we have committed a crime.

Put in this context, facial recognition raises a new constitutional question: do our faces deserve the same protection as our phones? From our perspective, the answer is a resounding yes.

VII. Looking beyond law and regulation

While we believe that new laws and regulations are indispensable, we also recognize that they are not a substitute for the responsibility that needs to be exercised by tech companies. Last December, we published ethical principles to govern Microsoft's facial recognition work.[55] These principles were developed after considerable input and advice from our employees, customers, public officials, academics and groups across civil society. This included incredibly helpful discussions both in the United States and around the world. The principles provide as follows:

1. ***Fairness.*** We will work to develop and deploy facial recognition technology in a manner that strives to treat all people fairly.
2. ***Transparency.*** We will document and clearly communicate the capabilities and limitations of facial recognition technology.
3. ***Accountability.*** We will encourage and help our customers to deploy facial recognition technology in a manner that ensures an appropriate level of human control for uses that may affect people in consequential ways.
4. ***Non-discrimination.*** We will prohibit in our terms of service the use of facial recognition technology to engage in unlawful discrimination.
5. ***Notice and consent.*** We will encourage private sector customers to provide notice and secure consent for the deployment of facial recognition technology.
6. ***Lawful surveillance.*** We will advocate for safeguards for people's democratic freedoms in law enforcement surveillance scenarios and will not deploy facial recognition technology in scenarios that we believe will put these freedoms at risk.

[55] See https://blogs.microsoft.com/on-the-issues/2018/12/17/six-principles-to-guide-microsofts-facial-recognition-work/.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

VIII. Moving Forward

Perhaps as much as any advance, facial recognition raises a critical question: what role do we want this type of technology to play in everyday society? As with any complicated issue, we readily recognize that we don't have all the answers regarding what kinds of rules and regulations ought to govern the use and development of facial recognition technology across society. In fact, given the early stage of facial recognition technology, we may not even know all the questions. But we firmly believe that government must act and determine what regulations that will permit the use of facial recognition technology to provide society with a whole host of benefits, while also addressing the challenges that facial recognition technology poses – challenges that go to the heart of fundamental human rights protections like privacy, freedom of expression, and freedom of association. Those challenges call for a thoughtful discussion including all stakeholders across society, and we stand ready to serve as a resource to help those discussions progress.

We would be happy to discuss this with you further and we look forward to working with you as your efforts progress. Thank you for your consideration.

Respectfully submitted,

Ryan P. Harkins
Senior Director, Public Policy
Microsoft Corporation

Appendix F

1. Special report – provided at first meeting https://www.ohioattorneygeneral.gov/Files/Publications-Files/General-Publications/Special-Reports/Facial-Recognition-Inquiries-Report_WEB
2. Pew Research Center, September 2019, "More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly" https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/
3. FISWG https://fiswg.org/index.htm
4. Indiana Intelligence Fusion Center's FR Policy https://www.in.gov/iifc/files/Indiana_Intelligence_Fusion_Center_Face_Recognition_Policy.pdf
5. Effectiveness of short-term FR training programs: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0211037
6. https://www.perpetuallineup.org/
7. MI-SNAP acceptable Use Policy 2016 https://www.michigan.gov/documents/msp/SNAP_Acceptable_Use_Policy_2016_03_07_533938_7.pdf
8. Law Enforcement Facial Recognition Use Case Catalog [IJIS Institute and the International Association of Chiefs of Police (IACP)] https://cdn.ymaws.com/www.ijis.org/resource/collection/93F7DF36-8973-4B78-A190-0E786D87F74F/Law_Enforcement_Facial_Recognition_Use_Case_Catalog.pdf
9. https://www.perpetuallineup.org
10. Garbage In, Garbage Out: Face Recognition on Flawed Data and America Under Watch: Face Surveillance in the United States. https://www.law.georgetown.edu/privacy-technology-center/publications/garbage-in-garbage-out-face-recognition-on-flawed-data/
11. https://www.flawedfacedata.com/
12. BJA Face Recognition Policy Development Template https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf
13. S.2878 – A bill to limit the use of facial recognition technology by Federal agencies, and for other purposes. https://www.congress.gov/bill/116th-congress/senate-bill/2878
14. NEC https://www.nec.com/en/global/solutions/biometrics/face/index.html
15. NIST Report https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

ATTACHMENT #1

OHIO ATTORNEY GENERAL FACIAL RECOGNITION TASK FORCE DRAFT REPORT & RECOMMENDATIONS

TO: Chairperson Sara Andrews and Facial Recognition Task Force members

FROM: Facial Recognition Task Force Members:
Jeremy Hansford, DPS/OSP Representative
Anne Dean, DPS/ BMV Representative

DATE: January 24, 2020

RE: DPS Comments

COMMENTS

The Ohio Department of Public Safety would like to comment on certain recommendations for clarification and with additional information, and respectfully request that these comments be recognized in the Report & Recommendation to the Ohio Attorney General.

Recommendation #3
The Attorney General should limit access to the Facial Recognition database to trained professionals at the Bureau of Criminal Investigation.

DPS recognizes and understands the benefits of centralizing facial recognition and limiting access to trained analysts, however, there is emphasis to ongoing concern from law enforcement on completing requests in emergency situations if a backlog develops that is too great for BCI analysts to manage.

Recommendation #6
The Attorney General should promulgate a specific standard for when law enforcement may utilize facial recognition, and this standard should require reasonable suspicion that the person to be identified has committed a crime, and should define investigative purpose.

DPS recommendations/comments:

1. A policy on responding to out-of-state law enforcement FR requests is needed as over 150 requests are currently pending a decision.
2. Appendix A Comments - Much debate was held on law enforcement reporting a disposition of each request. Concerns from law enforcement included the lack of inclusion on the disposition of a case once it is submitted to the prosecutor. Since facial recognition is used as a tool for

investigative leads only - the disposition from law enforcement should be limited to: (1) produced an investigative lead, or (2) failed to produce an investigative lead.

3. The Task Force agreed that demographic information for each probe photo evaluated should not be collected and stored as it could include racial bias or incorrect assumptions.

Recommendation #9
The facial recognition database system should adopt a reasonable image quality standard and disqualify images that do not meet that standard.

Per discussion in the Task Force meetings, BMV photos meet national standards for the issuance of driver license and identification cards, as is our core business, and such photos cannot be guaranteed to meet any established facial recognition standards due to inconsistency in photographic locations and lighting circumstances.

DPS requests that "image quality standard" be clearly defined as being used for purposes of investigation *after* enrolled in the facial recognition database, and that the BMV does not play a roll or have responsibility related to determining image quality.

Recommendation #11
The Attorney General should seek agreement from the Department of Public Safety and Bureau of Motor Vehicles to enroll current BMV images that meet the requisite image quality standard in the facial recognition database.

It is the request of DPS that Recommendation #11 be reworded to state the following: "The Attorney General should seek agreement from the Department of Public Safety and Bureau of Motor Vehicles to enroll current BMV images.", which better aligns with the last sentence of the recommendation's narrative that states "…images being imported is subject to agreement between the Attorney General and Department of Public Safety and consequently, the Task Force makes *no recommendation.*"

DPS requests that "image quality standard" be clearly defined as being used for purposes of investigation *after* enrolled in the facial recognition database, and that the BMV does not play a roll or have responsibility related to determining image quality.

Recommendation #13
The Attorney General should ensure the public has access to information about the use and regulation of facial recognition in Ohio.

DPS recommends the removal of the last sentence of this recommendation's narrative that talks about additional resources for public consumption, as edited below:

> *The Task Force understands the value of public education and the importance of finding ways to ensure the public has factual information about the use and regulation of facial recognition technology. In addition to the transparency suggestions included in Appendix B and Appendix C pursuant to Recommendation #13 and beyond posting rules, policy and regulations on a*

dedicated website for facial recognition, there should be features like Frequently Asked Questions (FAQ) to dispel myths and misunderstanding. ~~Additional resources for public consumption may include a list of terminology and definitions, notice that BMV images may be enrolled in the database and case profiles (generally) on how and in what situations the technology is used.~~

As there are many resources that could be made available, the intent would be to keep the recommendation broad and not set any specific and limited list of resources.

DPS further requests that the following information is available for consideration when allowing public access to information:

Concerns for undercover officer safety have come to our attention, which was not discussed by the Task Force. The BMV repository will contain images and identification information of current and future undercover officers. Facial recognition requests could unintentionally expose undercover officers by revealing their identity which could put them in danger. DPS is unable to remediate this risk outside the LEADS Trap, which is used to alert law enforcement of a hit on an undercover officer's information when a query is conducted against the live BMV repository.

CONCLUSION

On behalf of the Department of Public Safety, thank you for the opportunity to comment on the draft report and recommendation of the Task Force. Please note that any recommendations to DPS by this Task Force and/or the Attorney General are subject to additional review and approval by appointing authority.

[i] http://codes.ohio.gov/orc/109.57
[ii] https://www.law.georgetown.edu/privacy-technology-center/people/
[iii] https://www.nec.com/en/global/solutions/biometrics/face/index.html
[iv] http://files.ohleg.org/general/OHLEG_Rules_Regulations.pdf
[v] https://fiswg.org/index.htm
[vi] https://www.nist.gov
[vii] https://www.perpetuallineup.org
[viii] https://www.ohioattorneygeneral.gov/Law-Enforcement/Ohio-Law-Enforcement-Gateway
[ix] https://www.ohioattorneygeneral.gov/Files/Publications-Files/General-Publications/Special-Reports/Facial-Recognition-Inquiries-Report_WEB
[x] https://fiswg.org/index.htm
[xi] https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-and-criminal-history-record-training
[xii] http://files.ohleg.org/general/OHLEG_Rules_Regulations.pdf
[xiii] http://files.ohleg.org/general/OHLEG_Rules_Regulations.pdf
[xiv] https://www.perpetuallineup.org
[xv] https://fiswg.org/objectives.html
[xvi] https://www.nist.gov
[xvii] https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf
[xviii] https://www.sheriffs.org/sites/default/files/Whitepaper%20Facial%20Recognition.pdf
[xix] https://www.in.gov/iifc/files/Indiana_Intelligence_Fusion_Center_Face_Recognition_Policy.pdf
[xx] https://www.michigan.gov/documents/msp/SNAP_Acceptable_Use_Policy_2016_03_07_533938_7.pdf
[xxi] https://bja.ojp.gov/sites/g/files/xyckuh186/files/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf