

Article WaPo Facial Recognition.pdf

Uploaded by: David Moon

Position: FAV

Facial recognition firm Clearview AI tells investors it's seeking massive expansion beyond law enforcement

[washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition](https://www.washingtonpost.com/technology/2022/02/16/clearview-expansion-facial-recognition)

February 16, 2022

The facial recognition company Clearview AI is telling investors it is on track to have 100 billion facial photos in its database within a year, enough to ensure “almost everyone in the world will be identifiable,” according to a financial presentation from December obtained by The Washington Post.

Those images — equivalent to 14 photos for each of the 7 billion people on Earth — would help power a surveillance system that has been used for arrests and criminal investigations by thousands of law enforcement and government agencies around the world.

And the company wants to expand beyond scanning faces for the police, saying in the presentation that it could monitor “gig economy” workers and is researching a number of new technologies that could identify someone based on how they walk, detect their location from a photo or scan their fingerprints from afar.

The 55-page “pitch deck,” the contents of which have not been reported previously, reveals surprising details about how the company, whose work already is controversial, is positioning itself for a major expansion, funded in large part by government contracts and the taxpayers the system would be used to monitor.

The document was made for fundraising purposes, and it is unclear how realistic its goals might be. The company said that its “index of faces” has grown from 3 billion images to more than 10 billion since early 2020 and that its data collection system now ingests 1.5 billion images a month.

With \$50 million from investors, the company said, it could bulk up its data collection powers to 100 billion photos, build new products, expand its international sales team and pay more toward lobbying government policymakers to “develop favorable regulation.”

No federal law regulates how facial recognition should be used, though some cities and states have passed bans or restrictions. The biggest tech giants, including Amazon, Google, IBM and Microsoft, have limited or ended sales of the technology, saying they are worried about its risks or do not want to sell it to the public before Congress has established rules.

In the presentation, Clearview argues that the industry-wide caution is a huge business opportunity. The company included its rivals’ logos to note that it has little domestic competition — and that its product is even more comprehensive than systems in use in China, because its “facial database” is connected to “public source metadata” and “social linkage” information.

The presentation, which a recipient shared with The Post, throws a spotlight on the company's ambitions to become one of the world's leading merchants of surveillance technology, even as some lawmakers worry the company poses a dangerous threat to civil liberties and privacy rights.

Clearview has built its database by taking images from social networks and other online sources without the consent of the websites or the people who were photographed. Facebook, Google, Twitter and YouTube have demanded the company stop taking photos from their sites and delete any that were previously taken. Clearview has argued its data collection is protected by the First Amendment.

Facebook, which forbids the automated copying, or "scraping," of data from its platform and has an [External Data Misuse team](#), has banned Clearview's founder, Hoan Ton-That, from its site and has sent the company a cease-and-desist order, but Clearview has refused to provide any information about the extent to which Facebook and Instagram users' photos remain in Clearview's database, an official with Facebook's parent company, Meta, told The Post. The official declined to comment on any steps Meta may be considering in response.

Clearview's cavalier approach to data harvesting has alarmed privacy advocates, its peers in the facial recognition industry and some members of Congress, who this month urged federal agencies to [stop working with the company](#), because its "technology could eliminate public anonymity in the United States." Sens. Ron Wyden (D-Ore.) and Rand Paul (R-Ky.) last year [introduced a bill](#) that would block public money from going to Clearview on the basis that its data was "illegitimately obtained."

Clearview is battling a wave of legal action in state and federal courts, including lawsuits in California, Illinois, New York, Vermont and Virginia. New Jersey's attorney general has ordered police not to use it. In Sweden, authorities fined a local police agency for using it last year. The company is also facing a class-action suit in a Canadian federal court, government investigations in Canada, Sweden and the United Kingdom and complaints from privacy groups alleging data protection violations in France, Greece, Italy and the U.K.

The governments of [Australia](#) and [France](#) have ordered Clearview to delete their citizens' data, saying the company had covertly monetized people's faces for a purpose "outside reasonable expectations." "The indiscriminate scraping of people's facial images, only a fraction of whom would ever be connected with law enforcement investigations, may adversely impact the personal freedoms of all Australians who perceive themselves to be under surveillance," Australia's information and privacy commissioner, Angelene Falk, [said](#) in November.

Ton-That told The Post the document was shared with a "small group of individuals who expressed interest in the company." It included proposals, he said, not just for its main facial-search engine but also for other business lines in which facial recognition could be useful, such as identity verification or secure-building access.

He said Clearview's photos have "been collected in a lawful manner" from "millions of different websites" on the public Internet. A person's "public source metadata" and "social linkage information," he added, can be found on the websites that Clearview has linked to their facial photos.

Facial recognition companies have traditionally built algorithms that can be used to search through their clients' photo databases, such as driver's license images or jail mug shots. But Ton-That has argued in testimony to public officials that swiping photos from the Internet has allowed the company to create a powerful crime-fighting tool. "Every photo in the data set is a potential clue that could save a life, provide justice to an innocent victim, prevent a wrongful identification, or exonerate an innocent person," he said Wednesday in a statement to The Post, an echo of similar assertions he has made in public forums.

Clearview, he told The Post, does not intend to "launch a consumer-grade version" of the facial-search engine now used by police, adding that company officials "have not decided" whether to sell the service to commercial buyers.

If Clearview did decide to sell any technology to a nongovernmental buyer, Ton-That said, the company would first tell a federal court in Illinois, where Clearview is defending itself against class-action claims that it violated a state law requiring companies to obtain people's consent before collecting their facial data.

In a court filing Monday, U.S. District Judge Sharon Johnson Coleman, who is presiding over the case, upheld most of the plaintiffs' arguments challenging Clearview's work.

Clearview has dismissed criticism of its data collection and surveillance work by saying it is built exclusively for law enforcement and the public good. In an online "principles" pledge, the company said that it works only with government agencies and that it limits its technology to "lawful investigative processes directed at criminal conduct, or at preventing specific, substantial, and imminent threats to people's lives or physical safety."

But the presentation shows the company has based its "product expansion plan" on boosting corporate sales, from financial services and the gig economy to commercial real estate. On a slide devoted to its "total addressable market," government and defense contracts are shown as a small fraction of potential revenue, with other possible sources including in banking, retail and e-commerce.

Is there anything "they wouldn't sell this mass surveillance for?" asked Jack Poulson, a former Google research scientist who now runs the research advocacy group Tech Inquiry. "If they're selling it for just regular commercial uses, that's just mass surveillance writ large. It's not targeted toward the most extreme cases, as they've pledged in the past."

Clearview said in 2020 that it would stop working with private businesses after a BuzzFeed News report that found the company had offered its tool to stores, banks and other companies, including through 30-day free trials.

In his statement to The Post, Ton-That said: “Our principles reflect the current uses of our technology. If those uses change, the principles will be updated, as needed.”

Clearview clients can upload a photo to look for matches in the company’s face database, with the results often linking to the person’s other accounts across the Web. The company said its “index of faces” is now 11 times larger than the facial databases of “any government or nongovernment entity today.” (Many of the company’s claims in the document, including that one, could not be independently verified.)

Clearview was a little-known start-up until a New York Times report in early 2020, based on internal emails and public records uncovered by researchers, revealed the extent to which local police departments had begun using it to find potential suspects.

The company said it has since grown its client list to more than 3,100 law enforcement agencies in the United States. It has contracts with the Department of Homeland Security, the FBI and the Army.

Clearview has in the past year built up its executive ranks and advisory board with former high-ranking police and government officials. The company also has championed its work in helping to identify wanted criminals, including alleged rioters at the U.S. Capitol on Jan. 6, 2021.

But much of its new pitch to investors centers on its pursuit of the “limitless future applications” of nongovernment work, including in banking, health care, insurance and retail. “Everything in the future, digitally and in real life, will be accessible through your face,” the presentation says.

The company says in the presentation that it is hoping to raise \$50 million in a third round of investment, known as a “Series C.” The company raised \$30 million in a similar funding round last summer that valued the company at \$130 million.

Its relatively modest valuation, tech experts suggest, could be a reflection of the saturated market for facial recognition algorithms, the company’s precarious legal situation or the fact that its biggest selling point, its vast facial-data cache, has been called “illegitimately obtained.”

The company says in the presentation that it could “revolutionize” how workers in the gig economy are screened and that its technology could be used to evaluate people on apps used for dating or finding babysitters, house cleaners or repair contractors.

The presentation includes the logos for a number of companies, including Airbnb, Lyft and Uber. Ton-That said they were “examples of the types of firms that have expressed interest in Clearview’s facial recognition technology for the purposes of consent-based identity verification, since there are a lot of issues with crimes that happen on their platforms.”

Spokespeople at those three companies told The Post they had no plans to work with Clearview and had never expressed interest in a partnership.

Several other companies whose logos Clearview used as examples of potential business partners, including the babysitter service Sittercity, also said they had no plans to pursue any relationship with the company.

Justine Sacco, a spokeswoman with Tinder and OkCupid parent company Match Group, said that the companies have “never worked with Clearview AI and are not in any discussions with them” and that “Clearview is misusing our logo and does not have permission to use it in their materials.” An official at another company expressed anger over it being included in Clearview’s presentation and said it was considering legal options.

Clearview also says in the presentation that its systems could be used to solve “tough physical security problems” in retail and commercial real estate markets, and it included the logos of retail superstore companies such as Target and Walmart. Those companies did not immediately respond to requests for comment.

The company says in the presentation that it has developed other systems beyond facial recognition, including for recognizing license plates and “movement tracking,” and that it is developing or researching a number of other surveillance techniques: camera software to detect guns and drugs; “gait recognition” systems to identify a person based on how they walk; “image to location” systems to pinpoint a person’s whereabouts based on a photo’s background; and “contactless fingerprint” recognitions systems to scan a person’s identity from afar.

The document offers no details on how those systems work, if at all. Ton-That said the technologies “are all for the purpose of public safety, are in various stages of research and development, and have not been commercialized or deployed in any way.”

In an open letter last month, Ton-That said the company could “set an example of using the technology, *not in a real-time way*, but in a way that protects human rights, due process, and our freedoms.”

But the presentation directly contradicts him by saying the company is building systems for real-time surveillance. Officials are working toward a “real-time alerts” system that companies could use to notify security agents if it spotted “high-risk individuals,” one slide notes.

The company is also continuing work on augmented-reality glasses that the U.S. military could use in “dangerous situations,” one slide reads. The Air Force in November awarded the company \$50,000 to research the technology, federal spending records show. An official with the Air Force Research Laboratory has said the work is a short-term contract to test how well such technology would work.

In a September letter to the U.K. Surveillance Camera Commissioner office, Ton-That defended the use of real-time facial recognition watch lists for “people of interest, missing people, those with outstanding warrants for serious offenses, or for a specific security-related purpose known in advance.”

Clearview says in the presentation that its expansion plans would include spending millions of dollars more on data purchases and engineers specializing in data acquisition and that it would build out its teams specializing in commercial, federal and international sales. It says it also wants to create a “developer ecosystem” that would allow other companies to create applications using its data.

The company said that it expects to increase its annual federal revenue to \$6 million this year, thanks to active expansions with DHS and the FBI and an “imminent” expansion from the Drug Enforcement Administration, and that it hopes to “increase overall usage” by state and local police agencies by 300 percent.

U.S. Immigration and Customs Enforcement, a DHS agency, signed a one-year contract with Clearview in September that could extend to three years, totaling \$1.5 million, federal records show. The FBI signed an \$18,000 one-year contract in December; the presentation says it will grow to \$2.4 million this year. The DEA declined to comment, and the FBI and ICE did not respond to requests for comment.

The presentation also says Clearview is “achieving rapid international expansion,” including signing deals in Panama and Costa Rica and pursuing other business in Mexico, Colombia and Brazil. The company declined to offer further details, and those deals could not be confirmed.

The Clearview document includes overt appeals to American patriotism, and the company has, as is common among some tech companies, argued that its success is imperative to stopping foreign powers from gaining the lead in surveillance technology development. The company calls itself “Made in the USA” and, in several slides, compares itself with companies from China, Russia and Israel by affixing its logo next to an American flag.

But those arguments, Poulson said, should not distract from the company’s expanded ambitions — or its appetite for business far beyond the U.S. government’s interests.

“They’re explicitly trying to leverage the controversy about their company as a way to argue they’re prominent,” Poulson said. “And they’re combining that with a nationalist rhetoric — that the U.S. has to out-surveil China to protect civil liberties. It makes no sense.”

Aaron Schaffer contributed to this report.

HB 1046 support.pdf

Uploaded by: John Giannetti

Position: FAV

Maryland Criminal Defense Attorneys' Association



Md House of Delegates – Judiciary Committee

February 22, 2022

Hearing on HB 1046

Criminal Procedure – Facial Recognition Technology

MCDAA POSITION: SUPPORT

Brief bill explanation: This bill establishes significant new criminal law and criminal procedures regarding the use of facial recognition technology.

MCDAA's position: The use of facial recognition technology by law enforcement agencies must be carefully guided by the legislative bodies in our country. Significant civil liberties and privacy of Marylanders will be compromised without a careful examination of the use of this new technology. We generally endorse the aims and purposes of this legislation.

This legislation aims to limit the use of the technology to specific purposes: In connection with issuance of a warrant or at a preliminary hearing, and the results of the technology may not be used by the finder of fact as the sole basis to establish probable cause. Further, the bill significantly limits when the technology can be used during investigations and in analysis of videos or recordings of members of the public who are not the target of criminal investigations, and limits its use in real-time evaluation of images or recordings. We believe these are appropriate and needed limitations.

For additional information or questions regarding this legislation, please contact MCDAA Government Relations Contact John Giannetti 410.300.6393, JohnGiannetti.mcdaa@gmail.com

MOPD favorable with amendments hb 1046.pdf

Uploaded by: Andrew Northrup

Position: FWA



PAUL DeWOLFE
PUBLIC DEFENDER

KEITH LOTRIDGE
DEPUTY PUBLIC DEFENDER

MELISSA ROTHSTEIN
DIRECTOR OF POLICY AND DEVELOPMENT

KRYSTAL WILLIAMS
DIRECTOR OF GOVERNMENT RELATIONS DIVISION

ELIZABETH HILLIARD
ASSISTANT DIRECTOR OF GOVERNMENT RELATIONS DIVISION

POSITION ON PROPOSED LEGISLATION

BILL: HB 1046 - Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions

FROM: Maryland Office of the Public Defender

POSITION: Favorable with Amendments

DATE: 2/18/2022

The Maryland Office of the Public Defender respectfully requests that the Committee issue a favorable report on House Bill 1046 with the bill amended as below.

We would first like to thank and acknowledge Senator Sydnor for his persistence and determination in grappling with this issue over the last few years. This bill is an important first step in regulating the use of Facial Recognition Technology. The restriction of its use to the most serious crimes and the prohibition of its use at trial, will help to curtail the use of a potentially quite invasive technology. The Maryland Office of the Public Defender was involved in the workgroup assembled for this bill, and we support its purpose. After discussing the bill with others, however, certain shortcomings in the bill language became apparent. The understanding of certain provisions, while clear to the drafters, may not be so clear to later readers. To that end, we offer the following amendments.

First, to ensure transparency and to protect a criminal defendant's rights to due process and a fair trial it is imperative that a defendant is provided the results and supporting data whenever FRT is used. While Section 2-504 clearly states that the state shall disclose 'in accordance with the Maryland Rules regarding discovery.' In order to make clear that Facial Recognition Technology is addressed by the Maryland Rules of Discovery, it is our suggestion that a sentence be added to the end of the definition of Facial Recognition Technology at 2-501(B)(1) clarifying that Facial Recognition Technology is considered electronic surveillance for purposes of the rule.

Second, there appears to be agreement among all parties that the results generated from this technology should be used as an investigative lead and not introduced at trial under any circumstances. While there is language to this effect at the end of Section 2-503, it is our position that similar language should be added to the end of Section 2-502. Doing so would ensure that the use of this highly prejudicial, yet not quite generally accepted, technology would not be admitted at trial against an individual.

Additionally, under 2-506, in addition to posting the name and version of the Facial Recognition Software approved for use, DPSCS, should also post any developmental and internal validation studies conducted on that software so that communities can fully evaluate the technology. There is a large amount of mistrust around the misuse of surveillance technologies, and the use of them should be as transparent as possible.

Finally, it is important to recognize that this technology is new and is not as well understood as other technologies currently in use. Our understanding of the limits of this technology as well as of the ability of individuals to recognize faces accurately is not great. As our understanding of this area of science grows and standards are developed and accepted by the field, this legislation will almost certainly need to be revisited to incorporate these developments.

Nevertheless, this bill is an important first step to regulate this area of technology that has the potential to be highly invasive. We will tender to both sponsors amendments that we believe address the concerns that we have set forth above.

For these reasons, the Maryland Office of the Public Defender urges this Committee to issue a favorable report on the bill with the proposed amendments.

**Submitted By: Maryland Office of the Public Defender, Government Relations Division.
Authored By: Andrew Northrup, Forensics Division, (312) 804-9343,
andrew.northrup@maryland.gov.**

Microsoft Testimony - HB1046 OL.pdf

Uploaded by: Owen Larter

Position: FWA

HB1046 - Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions

FAVORABLE WITH AMENDMENT

Chairman Clippinger, Vice Chair Moon and members of the Judiciary Committee, my name is Owen Larter, I am Director of Public Policy in the Office of Responsible AI at Microsoft, thank you for the opportunity to submit testimony.

Microsoft would like to thank Senator Sydnor and Delegate Moon for their leadership on the issue of how to ensure facial recognition technology is used responsibly. This bill represents an important step forward in giving people protection under the law. Through this bill, Maryland has the opportunity to set itself apart as only the second state in the United States to establish specific guardrails to ensure that the use of facial recognition technology by law enforcement is rights-respecting, transparent, and accountable.

Facial recognition can provide many benefits to society, including helping secure devices and assisting people who are blind or with low vision access more immersive social experiences. In the public safety context, it can be used to help find victims of trafficking, or as part of the criminal investigation process.

However, without clear guardrails that have the force of law, facial recognition technology can also pose potential risks to individuals and society. There are three important types of potential risks around facial recognition technology:

- A risk of bias and unfair performance, including across different demographic groups;
- the potential for new intrusions on people's privacy; and
- possible threats to democratic freedoms and human rights.

Microsoft is clear-eyed about the potential risks that facial recognition can pose if not developed and used responsibly. Since 2018, we have engaged in an expansive program of work to design and enact effective safeguards to help secure its responsible use. This has included the internal adoption and implementation of Facial Recognition Principles¹ and the development of our Face API Transparency Note². The Transparency Note helps customers make informed decisions about how best to responsibly deploy our facial recognition service. It communicates, in understandable language aimed at non-technical audiences, how Face API works and the factors that will affect system accuracy. It also emphasizes the need to think about the whole system during deployment, including the importance of having a human in the loop.

In addition to these safeguards, Microsoft continues to believe that there is an urgent need for regulation. This need is particularly acute in the law enforcement context, given the consequential nature of the decisions that police take.

Microsoft strongly believes that facial recognition should not be deployed by police without specific civil liberties protections and safeguards in relation to transparency and accountability, testing, and human review. Microsoft believes this bill introduces some important safeguards, including:

- **Robust civil liberty protections**, such as restricting the use of facial recognition to establishing probable cause or positive identification in relation to only the most serious crimes, and only in conjunction with other independently obtained evidence. The prohibitions on real-time identification and the use of facial

¹ Microsoft, *Six Principles for Developing and Deploying Facial Recognition Technology*, <https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2018/12/MSFT-Principles-on-Facial-Recognition.pdf>.

² Microsoft AI, *Transparency Note: Azure Cognitive Services: Face API (2019)*, [https://azure.microsoft.com/mediahandler/files/resourcefiles/transparency-note-azure-cognitive-services-face-api/Face%20API%20Transparency%20Note%20\(March%202019\).pdf](https://azure.microsoft.com/mediahandler/files/resourcefiles/transparency-note-azure-cognitive-services-face-api/Face%20API%20Transparency%20Note%20(March%202019).pdf).

recognition on an individual suspected of being a juvenile provide further important protections, as does the prohibition on using the technology on the basis of an individual's engagement in constitutionally protected activity or their race, color, religious beliefs, sexual orientation, gender, disability, national origin or status as being homeless.

- **Transparency and accountability requirements**, such as the need for an agency to adopt a model policy on facial recognition use and a data management policy. It will be important that these policies are developed in a way that ensures police can identify and address risks around a system and keep data secure. The need to complete an annual audit to determine compliance with the law and use policies is also important, as is the restriction of facial recognition searches to high quality images in drivers' license and mugshot databases, which will deliver better quality results and provide transparency around the databases police are searching.
- **Important requirements around human review** of facial recognition output and the training and testing of the reviewer.

We do, however, think the bill can be strengthened, most notably by requiring two types of testing of facial recognition systems. First, the bill should require that vendors offering facial recognition services enable legitimate and reasonable third-party testing of their services. This is critical given the variation in accuracy across vendor offerings³. Third party testing is therefore needed to ensure law enforcement can identify and use more accurate systems that can be trusted by the public to perform well, including across different demographic groups.

Second, the bill should require agencies deploying facial recognition to subject those systems to operational testing prior to deployment in the environment in which they will be used. This is because environmental factors like lighting and camera positioning have a material impact on accuracy. Requiring that systems are tested and that any gaps in performance are addressed is therefore vital in ensuring police are using technology in a way that builds public trust.

Microsoft believes this bill represents important progress. We recognize that it is the product of an ongoing conversation between lawmakers, civil society, and law enforcement which we have welcomed the opportunity to contribute to. We look forward to continuing to contribute to this effort, now and in the future, with a view to building out safeguards for the responsible use of facial recognition that are robust and durable over the long term.

³ National Institute of Standards & Technology, Face Recognition Vendor Test (FRVT) (2022) 5, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

MCPA-MSA_HB 1046 Facial Recognition _Oppose.pdf

Uploaded by: Brian Carney

Position: UNF



Maryland Chiefs of Police Association

Maryland Sheriffs' Association



MEMORANDUM

TO: The Honorable Luke Clippinger Chairman and
Members of the House Judiciary Committee

FROM: Chief David Morris, Co-Chair, MCPA, Joint Legislative Committee
Sheriff Darren Popkin, Co-Chair, MSA, Joint Legislative Committee
Andrea Mansfield, Representative, MCPA-MSA Joint Legislative Committee

DATE: February 22, 2022

RE: **HB 1046 Criminal Procedure - Facial Recognition Technology -
Requirements, Procedures, and Prohibitions**

POSITION: **OPPOSE**

Since July 2021, the Maryland Sheriffs' Association (MSA) and the Maryland Chiefs of Police Association (MCPA) were pleased to participate with other stakeholders in a facial recognition working group formed by Senator Sydnor and Delegate Moon, at their request. Although there has been some productive dialogue over the last six months, the group has been unable to reach a consensus regarding a mutually agreeable bill. This has resulted in the production of a bill which restricts law enforcement's legitimate use of the technology and we feel it is imperative that changes be made to HB 1046. If changes are not made to this bill, public safety and crime victims could be adversely affected. Therefore, the MSA and the MCPA **OPPOSE HB 1046** in its current form.

Maryland law enforcement has successfully used facial recognition technology for many years. We recognize that there are misunderstandings surrounding facial recognition technology and its uses. There are many false narratives fueled by Hollywood portrayals which vastly misrepresent how law enforcement agencies legitimately use facial recognition. For example, facial recognition in Maryland is not used as ongoing government surveillance and it's not connected real time to live CCTV, Drone, Aviation or Body Worn Camera video. In reality, the facial recognition is primarily used in criminal investigations following an incident and under a process that requires a great deal of manual, human analysis, and an image of a sufficient quality to make a possible match.

The MCPA and MSA support the intention of the bill to establish safeguards for government use of the technology and we agree there should be use restrictions to ensure there is no intrusion on constitutionally protected activities. The successful use of facial recognition

technology in Maryland has aided in the identification of people whose images have been recorded on-camera committing robberies, burglaries, car jacking's, assaults, rapes, sexual assaults, shootings, homicides, kidnappings, hate crimes, human trafficking, sexual exploitation, threats of mass violence and other serious crimes. The technology has also been used to identify missing persons, deceased persons, incapacitated persons who can't identify themselves and to mitigate an imminent threat to health or public safety (e.g., to thwart an active terrorism scheme or plot).

The MCPA and MSA do not support the proposed amendments to this bill requiring the technology used by Maryland law enforcement to be made available to any third party for testing. The majority of facial recognition systems in use for law enforcement applications have algorithms which have been evaluated by the National Institute of Standards and Technology (NIST) for matching efficiency and accuracy, which includes an evaluation of the accuracy of the algorithm across demographics. Algorithms utilized for these systems are periodically updated as necessary based on subsequent NIST evaluations. The NIST Facial Recognition Vendor Test Program, located here in Gaithersburg, MD is already the world standard for independent, scientific evaluation of the technology.

Facial recognition is not an absolute science. It is not quantifiable like DNA, so while any potential match results will greatly contribute to the investigation, it will provide a tentative investigative lead only. When used in combination with human analysis and additional investigation, we have seen facial recognition technology is a proven valuable tool in solving crimes and increasing public safety.

We do not support HB 1046 mandating the use of a single facial recognition technology, which would limit photo sources to certain images which will have a clear and immediate negative impact on public safety. Due to the complexity of investigating crimes such as human trafficking and child sexual exploitation, there are some law enforcement agencies in the state using more than one facial recognition system, searching databases beyond driver's license, identification cards and booking photos. People who engage in this and other criminal activity often travel from out of state to commit crimes. Limiting use to a single facial recognition technology would prevent law enforcement from leveraging other legally obtained photos such as photos from other states and open-source photos which could assist with the identification of human trafficking/sexual exploitation victims, and individuals traveling from far outside the area to commit crime, as we saw with the unrest at the U.S. Capitol on January 6 last year.

We support ensuring that facial recognition alone does not constitute probable cause. However, it may generate investigative leads through a combination of biometric comparisons and human analysis. Investigators have to do the work, not the technology. The technology is used when there is already an investigation underway. We support that an arrest should not be made until the assigned investigator establishes, with other corroborating evidence, that the person identified by the photo match is the perpetrator in an alleged crime.

Facial recognition is a valuable time saving tool. Under traditional methods, law enforcement sought to identify an unknown person of interest during an investigation by manually looking through hundreds of mugshots with victims, canvassing areas with photos or searching a database using limited information. When time was crucial, the Anne Arundel County Police developed a tentative identification of the Capital Gazette shooter by using facial recognition technology to generate a lead. He was successfully identified, and later charged and convicted base

on other evidence. Let us not forget, when the need arose to expeditiously make tentative identification of persons involved in the unrest at the U.S. Capitol, the technology generated many investigative leads which when corroborated by additional investigative information led to the arrests and convictions of individuals who attacked our democracy.

The MCPA and MSA fully support strict guardrails and audit protocols to mitigate the risk of impartial and biased law enforcement and misuse of the technology, without eroding current investigative capabilities that have proven their worth. For example, we support the development of a model statewide use policy and ensuring relevant training in the use of the technology, as well as providing complete transparency through public reporting by agencies using the technology.

However, as currently drafted, HB 1046 contains several provisions that would unacceptably impact public safety in Maryland as well as hamper effective implementation of the requirements. We are unable to support the bill without key revisions. With the changes, HB1046 would be the strongest measure in the country for regulating the use of facial recognition technology used by law enforcement agencies, while addressing public concerns and preserving proven capabilities.

We applaud Co-Chair Moon and Senator Sydnor for their willingness to listen to participants in the facial recognition working group and we remain open to further discussion. However, HB 1046 as it stands limits the use of the technology, prevents human trafficking and juvenile victims from being identified and restricts law enforcement's ability to effectively investigate cases.

For aforementioned reasons, the MCPA and MSA OPPOSE HB 1046 and urge an UNFAVORABLE report.

Written Testimony (MD HB 1046SB 762).pdf

Uploaded by: Chris Johnson

Position: UNF

WRITTEN TESTIMONY OF DETECTIVE CHRIS JOHNSON

Reno Police Department

House Bill 1046 & Senate Bill 762 – Facial Recognition Technology

Thank you for the opportunity to provide this testimony. I am a detective with the Reno Police Department and I've seen first hand how facial recognition technology using an open source database can save the lives of exploited and abused children. Currently, I have been with the police department for over 9 years and have worked various assignments from patrol, being a field training officer, hostage negotiator, narcotics detective and now a detective assigned to investigate human trafficking assigned to the Regional Human Exploitation and Trafficking Unit (H.E.A.T).

Facial Recognition Technology Using an Open Source Database Saved a Trafficked Child

Detectives within Northern Nevada's Regional Human Exploitation and Trafficking Unit only had a few days to identify and save a child sexual exploitation victim before she left the city. The HEAT Unit monitors online prostitution ads to try and identify human trafficking victims. One ad in particular raised concern since the individual appeared to be a minor yet had facial tattoos—an unusual combination. We wanted to recover the victim from her trafficker before she moved from Reno to other major cities, but had no way to identify her. Online ads for prostitution do not use real names, and even the phone numbers are usually VoIP numbers that the police cannot associate with a known individual. Failure to rescue the victim while in Reno would expose the child to continued danger and possibly undermine established leads.

We then submitted one of the facial images from the ads in a facial recognition technology software that uses an open source database and within 10 to 15 seconds we had a possible lead, including a link to a publically available Instagram page. By researching the contents of the public Instagram profile, including comments on posts and other identifying information, we positively identified the victim within two hours of running the search—and also confirmed that she was a 16 year old juvenile. After this development, detectives conducted an undercover operation and recovered the victim from her trafficker, who was arrested that night.

At any given time, there may be thousands of prostitution advertisements posted online in a particular geographic region. This could imply a substantial amount of individuals are being

actively victimized. Law enforcement must in turn triage these potential victims, many of whom may be unidentified, with juvenile victims being the utmost priority in this process. Facial recognition technology offers law enforcement the ability to efficiently analyze images associated to these advertisements and determine the most critical victims requiring immediate law enforcement intervention.

Without the triage process and this technology which directly supports it, the 16 year old victim may not have been recovered.

Limiting the Database to the Motor Vehicle Division (MVA) and Mug Shots Would Have Resulted in Limited (if any) Leads

This 16 year old girl who was sex trafficked since she was 13 had no driver's license and no mug shot. If we had not used the open source database, we likely would have not rescued her at this point. And this is not a unique fact to her—many exploited children will not be found in MVA databases or mug shots. Furthermore, while it is critical for law enforcement agencies to have policies and procedures in place for the use of facial recognition technology, child trafficking cases move and change rapidly. Many of these children are moved from location to location on a regular basis. If we had waited for approval from another agency, which could take days or weeks and then had to wait again for the searches to be run—the 16 year girl would have been gone.

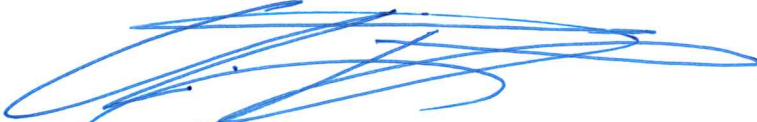
Facial Recognition Technology is One Piece of the Investigation

Within the HEAT Unit, facial recognition technology is used for after-the-fact investigations. Once we locate an image to use, we run it against the open source database. Then, human review and independent verification are a part of each search, so no automated decision-making is relied upon. Investigators will look through the publically available search results, verify the matches, and use them as leads.

Facial recognition technology using an open source database has the ability to save countless children from trafficking and exploitation—I've seen this first hand. However, limiting the

database to only MVA images and mug shots will significantly impair the power of this technology to save children. Using a database that uses publically available images is critical.

Thank you for your time.

A handwritten signature in blue ink, consisting of several overlapping, fluid loops and lines, positioned above the typed name.

Detective Chris Johnson

SIA Concerns - MD HB 1046 Facial Recongnition Techn

Uploaded by: Jacob Parker

Position: UNF



February 18, 2022

The Honorable Luke Clippinger
Chairman
House Judiciary Committee
Maryland House of Delegates
Annapolis, Maryland 21401

Written Testimony of SIA in Opposition to HB 1046, Regarding Facial Recognition Technology

Dear Chairman Clippinger and Members of the Judiciary Committee:

On behalf of the Security Industry Association (SIA) I am writing to express our concerns with House Bill 1046, as currently written. SIA is a nonprofit trade association in Silver Spring, MD that represents companies providing a broad range of security products and services in the U.S and throughout Maryland, including more than 30 companies headquartered in our state. Among many other companies, our members include the leading developers of facial recognition software available in the U.S., as well as those that integrate this technology into government, commercial and consumer products.

Support for Ensure Responsible, Ethical and Non-Discriminatory Use

We believe all technology products must only be used for purposes that are lawful, ethical, and non-discriminatory. Since many advanced technologies offer both tremendous benefits and the potential for misuse, we support policies ensuring facial recognition it is only used for appropriate purposes and in acceptable ways. Public concerns about facial recognition technology have centered around law enforcement and fears the technology might be used inaccurately or inappropriately, or in ways that raise privacy and civil liberties concerns. We believe establishing foundational safeguards in statute, combined with more detailed requirements in agency procedural rules, is the most effective approach to ensuring effective and accountable use of this technology by law enforcement over time. We support such policies consistent with SIA's *Principles for the Responsible and Effective Use of Facial Recognition Technology*,¹ and many thorough use policies put in place by leading agencies in Maryland and around the country.

HB 1046 Should Establish Rules, Not Eliminate Current Capabilities

While the intention of the bill is to establish safeguards for law enforcement use of the technology, several provisions eliminate current investigative tools being leveraged successfully by Maryland law enforcement. These are critical at a time of rising crime throughout the state, where shootings for example, have increased nearly 40% over the past year. The bill's limitation to queries against mugshot or driver's license photos using "a single facial recognition technology," would only serve to hamper and delay investigations versus provide any public benefit. Investigators routinely query open-source information and records held by other agencies to help identify victims, witnesses or suspects that may have no prior criminal history or are from outside Maryland, especially when other methods result in dead ends. As written the bill would prohibit one method – but not others – of analyzing the same available information. The prohibition on "live or real-time" use of the technology does not allow an exception for emergency situations when protecting lives demands being able to quickly identify a person of interest, such as during a terrorist attack. Additionally, the complete prohibition on queries to help identify minors will eliminate Maryland law enforcement

¹ <https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/>

capabilities essential to investigating human trafficking and child sexual exploitation. These harmful prohibitions in the bill simply must be removed to avoid a significant negative impact on public safety in Maryland.

Core Limitations and Transparency, Accountability Requirements

Facial recognition technology has been utilized by Maryland law enforcement for over a decade, without a single instance of misidentification, misuse or false arrest. Listed below in the appendix are just a few of many success stories. At the same time, there is a clear need for rules that help build public trust that technologies are being leveraged in a lawful, effective, accurate and non-discriminatory manner that benefits our residents and communities. We support the core provisions of the bill that address primary public concerns as well as impose stringent transparency and accountability requirements on agencies using the technology, which:

- **Prohibit law enforcement from using facial recognition match results as the sole basis to make an arrest, establish probable cause or make a positive identification.**
- **Ensure use of facial recognition technology in an investigation is discoverable in court proceedings.**
- **Exclude facial recognition results from use as evidence against a defendant.**
- **Prohibit use to analyze images of individuals engaged in constitutionally protected activities, or based solely on their race, color, religious beliefs, sexual orientation, gender, disability and national origin.**
- **Require a statewide standard for agency policies on use of the technology.**
- **Require annual reporting and periodic audits from agencies using the technology.**

Third-Party Testing

Additionally, we understand that an amendment may be offered that would require providers of technology used by Maryland law enforcement to make the same technology available to any “third party” for testing. Not only would this make it difficult, if not impossible for law enforcement to be able to obtain and use needed technology, it is completely unnecessary as facial recognition technologies for use for law enforcement applications have been evaluated by the U.S. Government’s National Institute of Standards and Technology (NIST). NIST tests and evaluates the speed, accuracy and performance of these technologies across a number of measurements including demographics. Algorithms utilized for these systems are periodically updated as necessary based on subsequent NIST evaluations. For over 20 years, the NIST Facial Recognition Vendor Test Program, located here in Gaithersburg, MD, remains the world standard for objective, third party scientific evaluation.

It is not clear what third parties are intended by the amendment or what objectivity or scientific expertise would be required. Developers of facial recognition for law enforcement use have generally not made their technology publicly available, to ensure it is only used for specific purposes and does not fall into the wrong hands. The requirement to provide an application programming interface (API) for third-party testing could also provide an unfair advantage to companies offering cloud-based “general purpose” software to the public. This requirement would disrupt agencies using technology that do not use cloud-based matching software – such as Maryland’s mugshot repository.

The Accuracy of Facial Recognition Technology

Calls for restricting use of the technology have often stemmed from misconceptions regarding its performance. While there is evidence that some, especially older versions of facial recognition technology have struggled to perform consistently across various demographic factors, the oft-repeated claim that it is *inherently* less accurate in matching photos of Black and female subjects simply does not reflect the current state of the science. In fact, the evidence *most* cited in the media is either irrelevant, obsolete, nonscientific or misrepresented.² An analysis of NIST test data in 2021 shows that each of the top 150 algorithms are over 99% accurate across Black male, white male, Black female and white female demographics, remarkable uniformity at high accuracy levels. For the top 20 algorithms,

² See - <https://www.securityindustry.org/2021/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/>

accuracy of the highest performing demographic versus the lowest varies only between 99.7% and 99.8%. For 17 of these algorithms, accuracy for white female, Black male and Black female are nearly identical at 99.8%, while they are least accurate for the white male demographic at 99.7%.³

The Case for Law Enforcement Use of Facial Recognition

In U.S law enforcement, facial recognition is used for a comparison search of records when the identity of the subject in an image is unknown, typically at the beginning stages of an investigation. It is used as a post-incident investigative tool to aid identification – not “surveillance.” The purpose is to generate or follow leads only and not to make a positive identification. Investigators compare “probe” images (such as photos lawfully obtained from a crime scene, no different from latent prints) against images in an established database for possible matches. However, unlike fingerprint and DNA matching, any potential facial recognition match result is not considered evidence. If an analyst using the software determines an image from a database likely matches a submitted image, investigators should use other means outside of facial comparison to provide confirming evidence needed to establish probable cause.

If the technology is not available, investigators will search arrest records by physical traits such as race and gender, as well as arrest history and other info, to narrow down search fields and possible identities before a visual examination of the photos in the records. However, as the importance of limiting human bias in police work becomes increasingly clear, biometric technology makes identification processes faster and more accurate than relying only on human analysis, subject descriptions, broadcasting suspect lookouts, public announcements or soliciting anonymous tips. Leading research⁴ tells us facial recognition is better at matching photos than humans can unassisted and that the highest accuracy results are achieved when combining technology and trained personnel.

Facial recognition has also been an indispensable tool for years in investigations of child sexual exploitation and human trafficking. There are several organizations that provide the technology to law enforcement investigators as part of tools developed for searching online information to make identifications in these cases. For example, the Thorn organization’s Spotlight tool is credited with helping rescue more than 17,000 children⁵ from trafficking over the last four years. According to the National Child Projection Task Force,⁶ facial recognition technology is key to its mission of bringing exploited children to safety and sexual predators to justice, as it assists investigations around the country.

Conclusion

On behalf of SIA and its members, we share the goal of ensuing responsible use of advanced technologies and would support policies ensuring that facial recognition is only used for appropriate purposes and in non-discriminatory ways. However, for the reasons above, we urge the Committee not to approve HB 1046 in its current form, and instead first work to correct the issues identified above. We stand ready to provide any additional information or expertise needed as you consider these issues.

Respectfully,



Jake Parker

Senior Director, Government Relations

Security Industry Association

Silver Spring, MD

jparker@securityindustry.org

³ *ibid.*

⁴ <https://www.nist.gov/news-events/news/2018/05/nist-study-shows-face-recognition-experts-perform-better-ai-partner>

⁵ <https://www.thorn.org/spotlight/>

⁶ <https://baltimore.legistar.com/View.ashx?M=F&ID=9438739&GUID=911C7E85-D97A-4325-A008-77AE42D1098E>

APPENDIX - MARYLAND SUCCESS STORIES

VICTIM IDENTIFICATION

- Following police response to a **shooting/robbery in Prince George's County, Maryland**, the victim could not be identified and remained in critical condition. Therefore, notification to his family had not been made. Images obtained from the victim's cell phone screen were queried and a lead was developed. Using other known images of the candidate, it was learned the candidate had a birth mark on his temple this information was shared with investigating officers who confirmed that the birthmark was present. The investigators were then able to contact the victim's family, and they responded to the hospital. While the victim ultimately succumbed to his injuries, quick work by investigators aided by facial recognition technology enabled the family to make it to the hospital before he passed.

RESPONDING TO HEALTH EMERGENCIES

- Maryland-National Capital Park Police responded to a **health emergency involving an individual at the College Park Airport**, with no shirt, shoes or mask, stating that they wanted to "fly to outer space/the stars" but the subject left the area before units arrived. An officer was able to locate the subject after subsequent calls from concerned citizens nearby; however, they had no identification and could not communicate coherently. An image was taken of the subject and queried, producing a potential matching female identity. At first, officers on the scene believed it was not a match because the individual was male. Upon further investigations the lead proved correct, as the transgender man's identity was confirmed by his father, who had been contacted in another state. The man had reportedly not been the same since taking LSD the previous week. He was reunited with a family member and then taken to a local hospital for evaluation.

PREVENTING IDENTITY THEFT

- A string of **fraudulent vehicle purchases in Montgomery County, Maryland**, were carried out using information obtained via identity theft, harming both the identity victims and dealerships that lost property. The suspects had created false identification documents used to purchase the vehicles, combining their own image with the personally identifiable information of a victim. These images were queried, leads were developed, and identities were confirmed through additional investigation and five arrests were made. Some of the suspects were arrested when they arrived to pick up a vehicle, since by that time they had already provided their false identification with their true image.

SOLVING VIOLENT CRIME

- Local law enforcement investigated a **violent assault on public transportation in Maryland**. Images of the suspect and the incident were obtained through video surveillance footage from the coach. Information was disseminated to law enforcement partners seeking assistance with the case. A comparison was made with regional booking and arrest photos. An investigative lead was developed and provided to the investigating agency, which upon further investigation led to the arrest of the assailant who was identified by the victim.

FIGHTING ORGANIZED CRIME AND GANG VIOLENCE

- Local **law enforcement in Maryland requested assistance with a firearms trafficking investigation**, providing an image of a suspect. The image was run against regional booking and arrest photos, and a potential lead was developed. Upon further investigation, detectives positively identified the suspect and executed a search warrant that resulted in the seizure of drugs, guns and ammunition.
- A retailer reached out to law enforcement with information about an **organized theft crew that had been targeting stores throughout Virginia, D.C. and Maryland**. An image provided showed a male with a rose tattoo on his neck and a skull tattoo on his left hand. The image against regional booking and arrest photos and a potential lead with the same tattoos was developed. Upon further investigation, the individual was subsequently identified and charged.

SIA Concerns - MD HB 1046 Facial Recongnition Techn

Uploaded by: Jacob Parker

Position: UNF



February 18, 2022

The Honorable Luke Clippinger
Chairman
House Judiciary Committee
Maryland House of Delegates
Annapolis, Maryland 21401

Written Testimony of SIA in Opposition to HB 1046, Regarding Facial Recognition Technology

Dear Chairman Clippinger and Members of the Judiciary Committee:

On behalf of the Security Industry Association (SIA) I am writing to express our concerns with House Bill 1046, as currently written. SIA is a nonprofit trade association in Silver Spring, MD that represents companies providing a broad range of security products and services in the U.S and throughout Maryland, including more than 30 companies headquartered in our state. Among many other companies, our members include the leading developers of facial recognition software available in the U.S., as well as those that integrate this technology into government, commercial and consumer products.

Support for Ensure Responsible, Ethical and Non-Discriminatory Use

We believe all technology products must only be used for purposes that are lawful, ethical, and non-discriminatory. Since many advanced technologies offer both tremendous benefits and the potential for misuse, we support policies ensuring facial recognition it is only used for appropriate purposes and in acceptable ways. Public concerns about facial recognition technology have centered around law enforcement and fears the technology might be used inaccurately or inappropriately, or in ways that raise privacy and civil liberties concerns. We believe establishing foundational safeguards in statute, combined with more detailed requirements in agency procedural rules, is the most effective approach to ensuring effective and accountable use of this technology by law enforcement over time. We support such policies consistent with SIA's *Principles for the Responsible and Effective Use of Facial Recognition Technology*,¹ and many thorough use policies put in place by leading agencies in Maryland and around the country.

HB 1046 Should Establish Rules, Not Eliminate Current Capabilities

While the intention of the bill is to establish safeguards for law enforcement use of the technology, several provisions eliminate current investigative tools being leveraged successfully by Maryland law enforcement. These are critical at a time of rising crime throughout the state, where shootings for example, have increased nearly 40% over the past year. The bill's limitation to queries against mugshot or driver's license photos using "a single facial recognition technology," would only serve to hamper and delay investigations versus provide any public benefit. Investigators routinely query open-source information and records held by other agencies to help identify victims, witnesses or suspects that may have no prior criminal history or are from outside Maryland, especially when other methods result in dead ends. As written the bill would prohibit one method – but not others – of analyzing the same available information. The prohibition on "live or real-time" use of the technology does not allow an exception for emergency situations when protecting lives demands being able to quickly identify a person of interest, such as during a terrorist attack. Additionally, the complete prohibition on queries to help identify minors will eliminate Maryland law enforcement

¹ <https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/>

capabilities essential to investigating human trafficking and child sexual exploitation. These harmful prohibitions in the bill simply must be removed to avoid a significant negative impact on public safety in Maryland.

Core Limitations and Transparency, Accountability Requirements

Facial recognition technology has been utilized by Maryland law enforcement for over a decade, without a single instance of misidentification, misuse or false arrest. Listed below in the appendix are just a few of many success stories. At the same time, there is a clear need for rules that help build public trust that technologies are being leveraged in a lawful, effective, accurate and non-discriminatory manner that benefits our residents and communities. We support the core provisions of the bill that address primary public concerns as well as impose stringent transparency and accountability requirements on agencies using the technology, which:

- **Prohibit law enforcement from using facial recognition match results as the sole basis to make an arrest, establish probable cause or make a positive identification.**
- **Ensure use of facial recognition technology in an investigation is discoverable in court proceedings.**
- **Exclude facial recognition results from use as evidence against a defendant.**
- **Prohibit use to analyze images of individuals engaged in constitutionally protected activities, or based solely on their race, color, religious beliefs, sexual orientation, gender, disability and national origin.**
- **Require a statewide standard for agency policies on use of the technology.**
- **Require annual reporting and periodic audits from agencies using the technology.**

Third-Party Testing

Additionally, we understand that an amendment may be offered that would require providers of technology used by Maryland law enforcement to make the same technology available to any “third party” for testing. Not only would this make it difficult, if not impossible for law enforcement to be able to obtain and use needed technology, it is completely unnecessary as facial recognition technologies for use for law enforcement applications have been evaluated by the U.S. Government’s National Institute of Standards and Technology (NIST). NIST tests and evaluates the speed, accuracy and performance of these technologies across a number of measurements including demographics. Algorithms utilized for these systems are periodically updated as necessary based on subsequent NIST evaluations. For over 20 years, the NIST Facial Recognition Vendor Test Program, located here in Gaithersburg, MD, remains the world standard for objective, third party scientific evaluation.

It is not clear what third parties are intended by the amendment or what objectivity or scientific expertise would be required. Developers of facial recognition for law enforcement use have generally not made their technology publicly available, to ensure it is only used for specific purposes and does not fall into the wrong hands. The requirement to provide an application programming interface (API) for third-party testing could also provide an unfair advantage to companies offering cloud-based “general purpose” software to the public. This requirement would disrupt agencies using technology that do not use cloud-based matching software – such as Maryland’s mugshot repository.

The Accuracy of Facial Recognition Technology

Calls for restricting use of the technology have often stemmed from misconceptions regarding its performance. While there is evidence that some, especially older versions of facial recognition technology have struggled to perform consistently across various demographic factors, the oft-repeated claim that it is *inherently* less accurate in matching photos of Black and female subjects simply does not reflect the current state of the science. In fact, the evidence *most* cited in the media is either irrelevant, obsolete, nonscientific or misrepresented.² An analysis of NIST test data in 2021 shows that each of the top 150 algorithms are over 99% accurate across Black male, white male, Black female and white female demographics, remarkable uniformity at high accuracy levels. For the top 20 algorithms,

² See - <https://www.securityindustry.org/2021/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/>

accuracy of the highest performing demographic versus the lowest varies only between 99.7% and 99.8%. For 17 of these algorithms, accuracy for white female, Black male and Black female are nearly identical at 99.8%, while they are least accurate for the white male demographic at 99.7%.³

The Case for Law Enforcement Use of Facial Recognition

In U.S law enforcement, facial recognition is used for a comparison search of records when the identity of the subject in an image is unknown, typically at the beginning stages of an investigation. It is used as a post-incident investigative tool to aid identification – not “surveillance.” The purpose is to generate or follow leads only and not to make a positive identification. Investigators compare “probe” images (such as photos lawfully obtained from a crime scene, no different from latent prints) against images in an established database for possible matches. However, unlike fingerprint and DNA matching, any potential facial recognition match result is not considered evidence. If an analyst using the software determines an image from a database likely matches a submitted image, investigators should use other means outside of facial comparison to provide confirming evidence needed to establish probable cause.

If the technology is not available, investigators will search arrest records by physical traits such as race and gender, as well as arrest history and other info, to narrow down search fields and possible identities before a visual examination of the photos in the records. However, as the importance of limiting human bias in police work becomes increasingly clear, biometric technology makes identification processes faster and more accurate than relying only on human analysis, subject descriptions, broadcasting suspect lookouts, public announcements or soliciting anonymous tips. Leading research⁴ tells us facial recognition is better at matching photos than humans can unassisted and that the highest accuracy results are achieved when combining technology and trained personnel.

Facial recognition has also been an indispensable tool for years in investigations of child sexual exploitation and human trafficking. There are several organizations that provide the technology to law enforcement investigators as part of tools developed for searching online information to make identifications in these cases. For example, the Thorn organization’s Spotlight tool is credited with helping rescue more than 17,000 children⁵ from trafficking over the last four years. According to the National Child Projection Task Force,⁶ facial recognition technology is key to its mission of bringing exploited children to safety and sexual predators to justice, as it assists investigations around the country.

Conclusion

On behalf of SIA and its members, we share the goal of ensuing responsible use of advanced technologies and would support policies ensuring that facial recognition is only used for appropriate purposes and in non-discriminatory ways. However, for the reasons above, we urge the Committee not to approve HB 1046 in its current form, and instead first work to correct the issues identified above. We stand ready to provide any additional information or expertise needed as you consider these issues.

Respectfully,



Jake Parker

Senior Director, Government Relations

Security Industry Association

Silver Spring, MD

jparker@securityindustry.org

³ *ibid.*

⁴ <https://www.nist.gov/news-events/news/2018/05/nist-study-shows-face-recognition-experts-perform-better-ai-partner>

⁵ <https://www.thorn.org/spotlight/>

⁶ <https://baltimore.legistar.com/View.ashx?M=F&ID=9438739&GUID=911C7E85-D97A-4325-A008-77AE42D1098E>

APPENDIX - MARYLAND SUCCESS STORIES

(shared by Maryland law enforcement agencies)

VICTIM IDENTIFICATION

- Following police response to a **shooting/robbery in Prince George's County, Maryland**, the victim could not be identified and remained in critical condition. Therefore, notification to his family had not been made. Images obtained from the victim's cell phone screen were queried and a lead was developed. Using other known images of the candidate, it was learned the candidate had a birth mark on his temple this information was shared with investigating officers who confirmed that the birthmark was present. The investigators were then able to contact the victim's family, and they responded to the hospital. While the victim ultimately succumbed to his injuries, quick work by investigators aided by facial recognition technology enabled the family to make it to the hospital before he passed.

RESPONDING TO HEALTH EMERGENCIES

- Maryland-National Capital Park Police responded to a **health emergency involving an individual at the College Park Airport**, with no shirt, shoes or mask, stating that they wanted to "fly to outer space/the stars" but the subject left the area before units arrived. An officer was able to locate the subject after subsequent calls from concerned citizens nearby; however, they had no identification and could not communicate coherently. An image was taken of the subject and queried, producing a potential matching female identity. At first, officers on the scene believed it was not a match because the individual was male. Upon further investigations the lead proved correct, as the transgender man's identity was confirmed by his father, who had been contacted in another state. The man had reportedly not been the same since taking LSD the previous week. He was reunited with a family member and then taken to a local hospital for evaluation.

PREVENTING IDENTITY THEFT

- A string of **fraudulent vehicle purchases in Montgomery County, Maryland**, were carried out using information obtained via identity theft, harming both the identity victims and dealerships that lost property. The suspects had created false identification documents used to purchase the vehicles, combining their own image with the personally identifiable information of a victim. These images were queried, leads were developed, and identities were confirmed through additional investigation and five arrests were made. Some of the suspects were arrested when they arrived to pick up a vehicle, since by that time they had already provided their false identification with their true image.

SOLVING VIOLENT CRIME

- Local law enforcement investigated a **violent assault on public transportation in Maryland**. Images of the suspect and the incident were obtained through video surveillance footage from the coach. Information was disseminated to law enforcement partners seeking assistance with the case. A comparison was made with regional booking and arrest photos. An investigative lead was developed and provided to the investigating agency, which upon further investigation led to the arrest of the assailant who was identified by the victim.

- The “**Capitol Gazette Killer**” **Jarroed Ramos** was angered by a story the *Capital Gazette* ran about him in 2011 and brought a lawsuit against the paper for defamation, which a judge later dismissed. In 2018, Ramos entered the newspaper’s headquarters in Annapolis, Maryland with a shotgun and killed five employees, leaving two others critically injured. Anne Arundel County Police faced a perfect storm of problems when they took the suspected gunman into custody: the man had no identification, he wouldn’t speak to investigators, and a fingerprint database was not returning any matches. They obtained an image of Ramos and sent it to the Maryland Combined Analysis Center, which helped identify him by comparing the photo to others in the Maryland Image Repository System.

SOLVING SEX CRIMES

- In Glen Burnie, MD, a former Metropolitan Police Officer was indicted on charged of sex trafficking of minors and enticement of minors to engage in prostitution, involving sexual contact with two minor girls. Use of facial recognition technology provided a lead that helped solve the case.

FIGHTING ORGANIZED CRIME AND GANG VIOLENCE

- **Local law enforcement in Maryland requested assistance with a firearms trafficking investigation,** providing an image of a suspect. The image was run against regional booking and arrest photos, and a potential lead was developed. Upon further investigation, detectives positively identified the suspect and executed a search warrant that resulted in the seizure of drugs, guns and ammunition.
- A retailer reached out to law enforcement with information about an **organized theft crew that had been targeting stores throughout Virginia, D.C. and Maryland.** An image provided showed a male with a rose tattoo on his neck and a skull tattoo on his left hand. The image against regional booking and arrest photos and a potential lead with the same tattoos was developed. Upon further investigation, the individual was subsequently identified and charged.

HB1046 - Facial Recognition .pdf

Uploaded by: Jennifer Beskid

Position: UNF



Department of Public Safety and Correctional Services

Office of Government and Legislative Affairs

45 Calvert Street, Suite 7A-C, Annapolis MD 21401
410-260-6070 • www.dpsscs.state.md.us

STATE OF MARYLAND

LAWRENCE J. HOGAN, JR.
GOVERNOR

BOYD K. RUTHERFORD
LT. GOVERNOR

ROBERT L. GREEN
SECRETARY

RACHEL SESSA
CHIEF OF STAFF

SASHA VAZQUEZ-GONZALEZ
ACTING DEPUTY SECRETARY
ADMINISTRATION

WAYNE HILL
DEPUTY SECRETARY
OPERATIONS

CAROLYN J. SCRUGGS
ASSISTANT SECRETARY

GARY McLHINNEY
ASSISTANT SECRETARY

JENNIFER A. BESKID
DIRECTOR

BILL: HOUSE BILL 1046

POSITION: OPPOSE

EXPLANATION: This bill establishes requirements and procedures relating to the use of facial recognition. Further, the bill requires the Department to adopt and publish a statewide model policy and develop and administer a training program regarding the use of facial recognition.

COMMENTS:

- The Department of Public Safety and Correctional Services operates the State's prisons that house individuals sentenced to serve 18 months or longer. The Department also oversees the Division of Parole and Probation, which supervises individuals who are on parole or probation in the community. The Department also runs the Baltimore City Pretrial Complex that houses individuals awaiting trial.
- The Department houses the facial recognition program. The approximately 150 law enforcement agencies in the State use this tool to aid in the investigation of unknown individuals. It is up to each law enforcement agency to determine the circumstances of its use.
- Section 2-506 of the bill will require the Department to:
 - Adopt and publish a model statewide policy regarding the use of facial recognition.
 - Develop and administer a training program as well as proficiency testing as it pertains to the use of facial recognition technology in the courts and criminal investigations - including training and testing on cultural diversity and implicit bias.
 - **Review and approve a single facial recognition technology for use by law enforcement agencies in the State.**
- **The Department is concerned with the language in Section 2-506 as it is not in a position to determine the best and sole facial recognition technology for the approximately 150 law enforcement agencies in the State;** especially as the Department is not aware of the technology maintained by each agency and its compatibility with existing facial recognition technology.

- Additionally, the bill states a law enforcement agency may not use or contract for the use of facial recognition technology for use in criminal investigations unless the technology is currently approved for use by the Department. As stated previously, the Department does not have knowledge of the technological capabilities of various law enforcement agencies nor is the Department able to determine what is the best resource for EACH agency when conducting criminal investigations.
- The Department of Public Safety and Correctional Services is NOT a law enforcement agency. As such, the Department should not drive policy on how law enforcement agencies use facial recognition, including approving what technology is used.
- The Department understands amendments to the bill may be forthcoming that would address the Department's concerns and could be supported.

CONCLUSION: For these reasons, the Department of Public Safety and Correctional Services respectfully requests the Committee vote **UNFAVORABLE** on House Bill 1046.

Written Testimony Kevin Metcalf (Maryland HB 1046_

Uploaded by: Kevin Metcalf

Position: UNF

WRITTEN TESTIMONY OF KEVIN METCALF

National Child Protection Task Force (NCPTF)

House Bill 1046 & Senate Bill 762 – Facial Recognition Technology

Thank you for the opportunity to provide this testimony. Since February 2011, I have been a Deputy Prosecuting Attorney at the Washington County Prosecutor's Office in Arkansas, where I prosecute felonies. I am also the founder and Chief Executive Officer of National Child Protection Task Force (NCPTF). The NCPTF is a non-profit organization with approximately 50 volunteers that include active-duty law enforcement officers who volunteer their time to help state, federal, and international law enforcement agencies investigate online child abuse, recover exploited children, and hunt sexual predators and human traffickers.

The members of the NCPTF help provide detectives, analysts, and officers access to investigative expertise and resources that are unavailable or underfunded in most law enforcement organizations. For example, the NCPTF brings together recognized experts in facial recognition technology, strategic legal applications, open-source intelligence, cellular mapping and analysis, dark-web investigations, and cryptocurrency to aid law enforcement agencies everywhere. Through my work as a prosecutor and with the NCPTF, I have assisted with the recovery of hundreds of missing and exploited children and helped identify and apprehend hundreds of sexual predators in multiple states and countries.

Open-source intelligence is a critical component in the timely identification and rescue of these young victims of violent crimes. In fact, without the ability to effectively process open-source intelligence, our success in these cases would be tragically impaired. I could give you hundreds of examples of children who were being sexually exploited or raped and were rescued solely because of access to open-source intelligence, but most cases follow the same general fact pattern. Law enforcement officers find videos and photos on the dark web of children being raped -- many are produced by parents, siblings, or other close family members. Law enforcement knows nothing about these children other than the fact that they are being raped and that their videos and photos are being traded or sold on the dark web.

Using traditional investigative techniques, law enforcement officers have to carefully scrutinize every second of these rape videos hoping that the perpetrators will make a mistake and reveal a clue, such as a street sign, identification card, or receipt that could give investigators a lead. On the dark web, predators maintain manuals of changes in the law, technological advances, and the methods investigators use to identify other pedophiles. The ready availability of these how-to manuals means that predators make fewer mistakes that investigators can use to track them, and children continue to be exploited and raped.

Most of the time, law enforcement only has images of helpless children's faces with no way to identify them or bring them to safety. It is fruitless to run the faces of child rape victims, many of whom are prepubescent, through traditional law enforcement facial recognition programs because these programs are typically limited to booking photos. Sometimes, the faces of predators are present, but that is still a long shot as many of the abusers have managed to avoid arrest.

We must use open-source intelligence to identify these victims and these perpetrators. And the best source of this intelligence is publicly available data and images from the internet. But as you can imagine, the vastness of the public internet makes it impossible to effectively search it by a single human investigator or even a team of investigators. It requires working collaboratively with companies that aggregate public data and publicly available images. The data they provide is data that I or any investigator in the world would already have lawful access to, but it would take months, even years, to effectively search it manually. These young victims don't have months or years, some don't have hours, before they are violated again, so there is a real urgency in the need to quickly identify the victims and suspects in these cases. The use of modern, high-performing facial recognition technology and aggregated public data and images are crucial to our continued success.

This technology and publicly available dataset helps protect children who would otherwise slip through the cracks -- children who have not been reported as missing or abused and are being raped by their parents, family members, or others close to the child.

Example of Locating Child Using FRT

In one case here in the U.S., a predator was posting images of the sexual abuse of very young children; the images indicated he had access to children and was actively raping and abusing them. However, one of the pictures he posted included the face of a young teenage girl. Using technology with an open-source database, investigators were able to identify the girl from an old Instagram account she no longer used. This allowed law enforcement to find her and identify the predator, who was actively abusing very young children. This teen's face would not appear in a driver's license database or booking photos.

MVA Database and Mug Shots Severely Limit Effectiveness of FRT in Child Exploitation Cases

Despite the misinformation out there on this subject, high-performing facial recognition technology is extremely accurate, and when used within appropriate procedures and guidelines is very effective. Facial recognition offers unprecedented capabilities to identify stalkers, rapists, child abusers, and other online predators and could facilitate identification of previously unknown child victims depicted in child sexual-abuse material proliferating online. However, limiting the data set to only that provided by the motor vehicle administration (MVA) is extraordinarily limiting. This will not help identify a deceased child, a minor victim, or a suspect traveling through the state that is not in the MVA data set. The issues related to limiting law enforcement's data set are infinite. Limiting the dataset to only MVA images and mug shots significantly increases the likelihood of misidentifications and completely omits the important work being done with facial recognition to identify children who are abused and whose images appear online.

Open-source data has been a game changer for rescuing and identifying victims such as children and identifying violent criminals that are from other states and countries. Law enforcement has

significantly increased the rate of identifying child victims of sexual abuse online using platforms of aggregated publicly available data and images.. In fact, limiting datasets has many unintended consequences, aside from severely limiting its use in child exploitation cases. Restricting a law enforcement agency to look for perpetrators in criminal datasets such as mug shots is inherently biased in itself. It encourages the resolution of crimes that point to repeat offenders and discourages resolution of investigations involving unknown persons that are not in the typical local data set. Citizens should be concerned if the only data its law enforcement is permitted to use is that of its own communities.

In many investigations, but more so related to children, time is never on the side of law enforcement. While reasonable and effective policies and procedures are critical for law enforcement's use of facial recognition technology, limiting the databases or creating a complicated process where it could take days, weeks or months to use the technology could mean another child is lost. Trafficking and crimes against children move quickly. A child being sex trafficked could be in one location and then moved to another state the following day (or even that same day). If law enforcement cannot use facial recognition technology promptly because an investigator has to place multiple requests, has to obtain approval from another agency or department, and then waiting for days for a search to be returned – it will be too late, the child will be in another location.

Without facial recognition technology that uses a database of publicly available data and images , we will lose the ability to save hundreds of children from continuing to be raped, and these recordings shared on the internet for the world to see. Further, limiting law enforcement's ability to use facial recognition technology and limiting it to the MVA dataset will significantly curtail the success of law enforcement in cases where the children are victims.

Thank you for your time.

Kevin Metcalf

MSP Position Paper for HB1046.pdf

Uploaded by: Thomas Williams

Position: UNF



State of Maryland
Department of State Police
Government Affairs Section
Annapolis Office (410) 260-6100

POSITION ON PROPOSED LEGISLATION

DATE: February 22, 2022

BILL NUMBER: House Bill 1046 **Position:** Oppose/Amendments

BILL TITLE: Criminal Procedure – Facial Recognition Technology – Requirements, Procedures, and Prohibitions

REVIEW AND ANALYSIS:

This legislation seeks to establish requirements, procedures and prohibitions for the use of facial recognition technology (FRT) by a law enforcement agency. The legislation further seeks to define FRT and require certain training and testing proficiency.

The Department of State Police (DSP) was grateful to be a part of a workgroup looking into the use of FRT. The workgroup discussed a number of issues including how FRT is deployed today. One goal of the DSP was to keep any legislation on the use of FRT simple and provide guidelines that would allow the technology to be used as an investigative tool, limiting its use in court, providing a model policy, and preventing misuse. While some of our recommendations made it into the legislation, the bill in its current form causes concern.

Section 2-503 limits the use of FRT to identify a person suspected of being a juvenile who is ineligible to be charged with a criminal act. This restriction eliminates the possibility of identifying certain juveniles involved in serious crimes. With serious juvenile crime prevalent in many locations we should not be limiting a public safety investigative tool which could provide the identity of a suspect. Striking this restriction ensures Maryland Law enforcement can continue to leverage tools essential to crime solving, human trafficking and child sexual exploitation investigations.

This section also limits the FRT queries to the Maryland Motor Vehicle Administration or other state DMV images and mug shots maintained by local, state or federal law enforcement agencies. As previously mentioned, juveniles are involved in a host of crimes. Many are not in the mug shot databases nor do they have driver's licenses. This limitation also extends to the search for missing children, human trafficking victims, missing adults, etc. The limitation prohibits the technology from accessing this state or other state's sex offender websites, the Maryland and National Center for Missing and Exploited Persons images, wanted posters or other images posted by law enforcement or families. Striking these limitations will allow law enforcement investigators to use FRT to possibly identify individuals with no prior criminal history, do not have an ID card or driver's license, non-MD residents or minors, who are suspects or unidentified victims.

Section 2-506 requires the Department of Public Safety and Correctional Services (DPSCS) to develop a model policy, administer a training program and provide proficiency testing regarding the use of FRT. Some of the agreements we thought were reached in the workgroup are training should be specific to the vendor and the technology used, proficiency testing would not be required because the results are inadmissible in court, and the DSP would be responsible for the model policy. In concert with this, DSP supported the results generated by the FRT to be reviewed by an independent person.

State of Maryland
Department of State Police
Government Affairs Section
Annapolis Office (410) 260-6100

POSITION ON PROPOSED LEGISLATION

Although there are a number of other problems with HB1046, one of the most important restrictions that should be struck is the requirement that the DPSCS review and approve a single FRT for use by law enforcement agencies. This restricts over 156 police agencies to one technology regardless of the system's limitations or the local department's needs. It eliminates local control and places the burden on DPSCS to review and approve a single technology.

What is most interesting about the restrictions posed by the legislation is, today, law enforcement can take a photo and send it to news outlets, post it on any platform using the internet, or circulate it to a targeted area to try and identify an individual(s) suspected of a crime, or try to identify an unidentified person or victim, as part of a legitimate investigation, to get human input into the identity of the person. But, if law enforcement tries to use FRT as a tool, somehow, we have violated someone's rights.

There are a number of additional amendments DSP would like to see made to this legislation. DSP will continue to work with the sponsor to develop additional amendments to the legislation.

For these reasons, the Department of State Police urges the Committee to give House Bill 1046 as written an unfavorable report.