MEMO

DATE: May 6, 2024

TO: Police Accountability Commission

FROM: Kelly Stachowicz, Assistant City Manager

SUBJECT: Information from Facial Recognition Technology Subcommittee

---

In February, the Police Accountability Commission began a discussion on facial recognition technology. The discussion continued at the March and April meetings, with a subcommittee of Cecilia Escamilla-Greenwald, Dillan Horton, and John Myers to look further into the use of facial recognition technology by law enforcement and to return to the full Commission with feedback and recommendations.

The Commission received materials from the subcommittee in April. Attached to this memo are additional materials from the subcommittee for the May meeting.

These items are presented as submitted and have not been reviewed by staff or the City's legal counsel.

In addition to the information presented by the subcommittee, public and additional commissioner communication that has been submitted to the PAC since the last meeting has been included in the packet with this item.

Attachments

1. Slide presentation from subcommittee
2. Draft ordinance from subcommittee
3. Communications (public, commissioner)

Considerations on Prohibiting FRT in Davis Policing

Davis Police Accountability Commission

Previous Cases of False Match

Houston - Harvey Eugene Murphy Jr

Murphy was accused and arrested for robbing thousands of dollars of merchandise from a Sunglass Hut in the surrounding houston area. He was in Sacramento, CA at the time of the robbery. While in jail, he was sexually assaulted. He also did have criminal record, but had a new, clean life.

Jefferson Parish - Randal Quran Reid

Reid was arrested and held for a week on a warrant issued in Louisiana. Reid kept stating how he had never been to Louisiana. Officers of the Jefferson Parish Sheriff's Office used FRT to identify Reid. It was believed he used stolen cards to purchase $15,000 worth of designer purses.

Detroit - Porsche Woodruff

Police officers came to Woodruff's home to arrest her for robbery and carjacking. She was eight months pregnant during the arrest, and began having pains. She was released on $100,000 bail. At the time she was the sixth person to be incorrectly identified from FRT in Detroit.

Previous Cases of False Match

Rite Aid - 11 year old

Rite Aid had a database made of cameras, employee phones, news stories, etc. Due a false match, a 11 year-old girl had to be searched by an employee. She was so distraught she and her mother had to take time of school and work respectively

Woodbridge - Nijeer Parks

Parks was released on drug-related charges and had clean, stable life now. The Woodbridge police used a facial recognition scan on a fake ID left at a crime scene. Parks was charged with aggravated assault, unlawful possession of weapons, using a fake ID, possession of marijuana, shoplifting, leaving the scene, resting arrest and an accusation of almost hitting an officer with a car

Detroit - Robert Williams

Williams was arrested on a robbery charge. Williams at the time was a 43-year-old father. They held him in interrogation for 30 hours, however, during the robbery he was driving home. The Police chief even said the investigative work “shoddy”. William’s image from a dimly lit surveillance camera was used of FRT. According to his attorney’s, his daughters were traumatized from the incident

Facial Recognition Technology (FRT) Accuracy and Demographic Disparities

-
- UK's Metropolitan Police: Out of 104 alerts generated by FRT, only 2 resulted in positive matches, indicating a low accuracy rate.
- South Wales Police: FRT produced correct matches in less than 10% of cases, raising concerns about its reliability.
- Oxford St., London: FRT exhibited its lowest accuracy rates when identifying individuals of Black ethnicity, highlighting potential racial biases.
- Latinx ethnicities were notably absent from the testing process, prompting questions about inclusivity and representation in FRT testing.
- False Positive Rates:
    - Groups most affected by false positives were Black individuals, males, and younger age groups, Conversely, White individuals and those over the age of 42 experienced almost no false matches, indicating disparities in FRT accuracy across demographic groups.

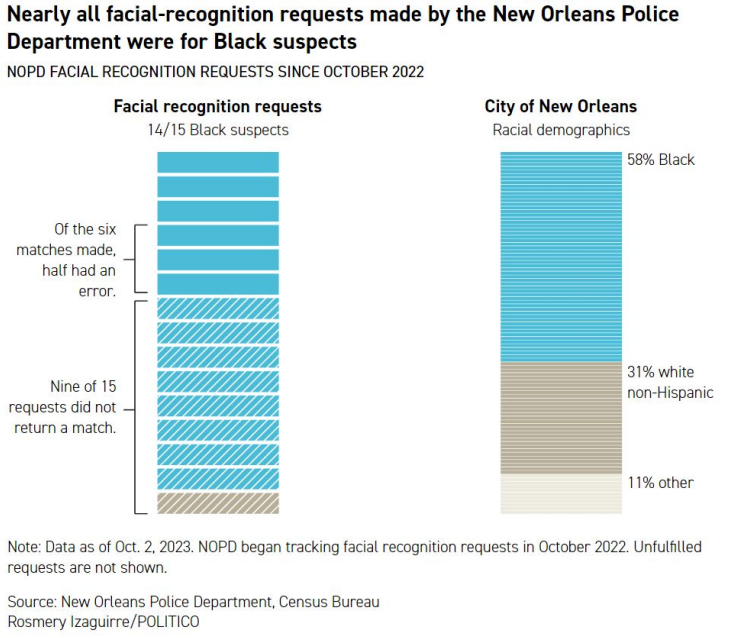
Table 6 — Number of Cohort subjects with false positive by Gender, Ethnicity & Age

Face-match threshold Face-detection settings	FPIR	Female	Male	Asian	Black	White	Age <21	Age 21-30	Age 31-42	Age >42
0.64 (a)	0.00 %	0	0	0	0	0	0	0	0	0
0.62 (a)	0.05 %	1	0	0	1	0	0	1	0	0
0.60 (a)	0.25 %	2	4	2	4	0	0	5	1	0
0.60 (b)	0.30 %	2	5	4	3	0	0	7	0	0
0.58 (a)	0.48 %	7	8	4	11	0	2	9	3	1
0.56 (a)	1.15 %	16	17	8	22	3	7	18	7	1
Recognition opportunities: gender, ethnicity & age balance		51%	49%	26%	29%	45%	26%	26%	24%	24%

Notes:
Watchlist size:178,000
Recognition opportunities: 4000

Effectiveness and Misidentification Issues with FRT in Law Enforcement

- New Orleans Police: Only 3 potentially correct matches were identified through FRT usage over the course of a year, indicating low effectiveness.
- Out of 19 felony cases submitted for FRT processing, only 15 were processed, with 12 resulting in incorrect or unusable matches, underscoring reliability concerns.
- Detroit Police Chief acknowledges a 96% rate of incorrect matches with FRT, highlighting significant flaws in the technology's accuracy.
- FRT was employed 70 times by Detroit police, with 68 instances involving individuals of Black ethnicity, exacerbating concerns about racial bias and accuracy disparities within FRT usage.



'Wholly ineffective and pretty obviously racist': Inside New Orleans' struggle with facial recognition policing by Alfed NG

Microsoft's Facial Recognition Technology (FRT) Error Rates

- Microsoft: Reports a 6.3% error rate with its FRT technology, indicating significant room for improvement.
- Notably, there is a stark disparity in error rates based on gender and skin tone:
  - Females with dark skin experience an error rate of 20.8%, significantly higher than the 1.7% error rate observed for males with light skin.
- While the overall error rate may appear relatively low, it fails to capture the disproportionate impact on already marginalized groups.
- FRT's high inaccuracy rates for oppressed groups raise ethical and social concerns regarding fairness and equity in technology usage.
-

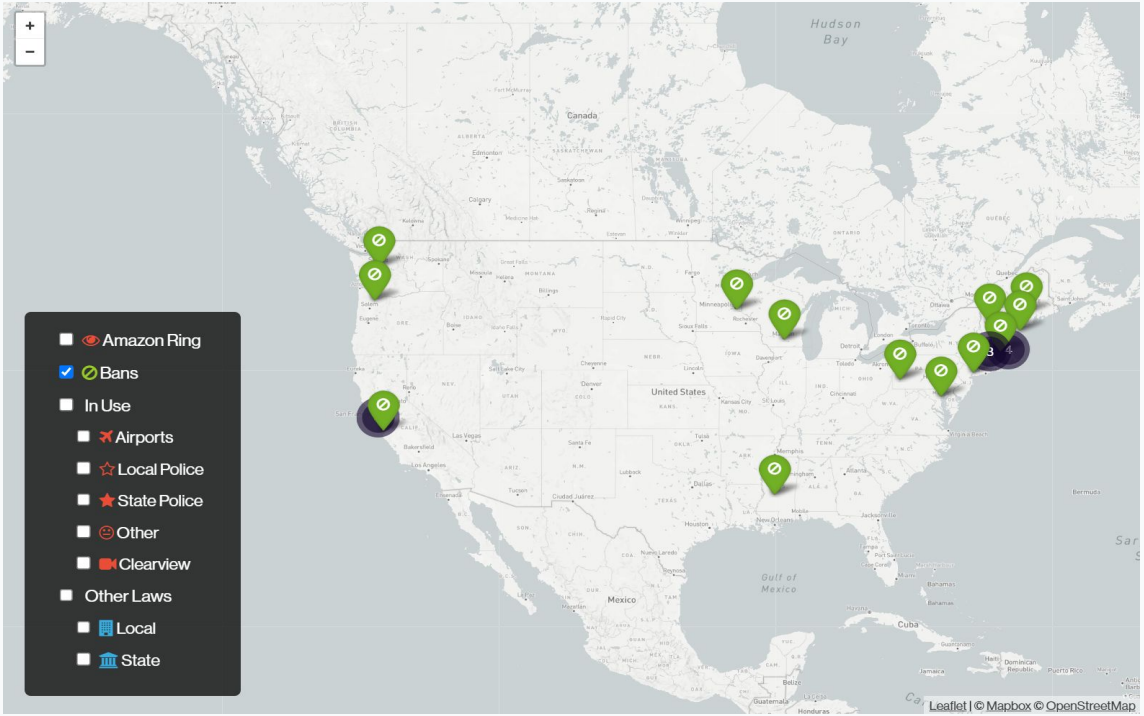
Classifier	Metric	All	F	M	Darker	Lighter	DF	DM	LF	LM
MSFT	TPR(%)	93.7	89.3	97.4	87.1	99.3	79.2	94.0	98.3	**100**
	Error Rate(%)	6.3	10.7	2.6	12.9	0.7	**20.8**	6.0	1.7	0.0
	PPV (%)	93.7	96.5	91.7	87.1	99.3	92.1	83.7	**100**	98.7
	FPR (%)	6.3	2.6	10.7	12.9	0.7	6.0	**20.8**	0.0	1.7
Face++	TPR(%)	90.0	78.7	99.3	83.5	95.3	65.5	**99.3**	90.2	99.2
	Error Rate(%)	10.0	21.3	0.7	16.5	4.7	**34.5**	0.7	9.8	0.8
	PPV (%)	90.0	98.9	85.1	83.5	95.3	98.8	76.6	**98.9**	92.9
	FPR (%)	10.0	0.7	21.3	16.5	4.7	0.7	**34.5**	0.8	9.8
IBM	TPR(%)	87.9	79.7	94.4	77.6	96.8	65.3	88.0	92.9	**99.7**
	Error Rate(%)	12.1	20.3	5.6	22.4	3.2	**34.7**	12.0	7.1	0.3
	PPV (%)	87.9	92.1	85.2	77.6	96.8	82.3	74.8	**99.6**	94.8
	FPR (%)	12.1	5.6	20.3	22.4	3.2	12.0	**34.7**	0.3	7.1

Table 4: Gender classification performance as measured by the positive predictive value (PPV), error rate (1-TPR), true positive rate (TPR), and false positive rate (FPR) of the 3 evaluated commercial classifiers on the PPB dataset. All classifiers have the highest error rates for darker-skinned females (ranging from 20.8% for Microsoft to 34.7% for IBM).

Gender Shade: Intersectional Accuracy Disparities in Commercial Gender Classification By Joy Buolamwini and Timnit Gebru

Other Legislation Being Done

- Many cities with similar political standing to Davis have implemented full bans or have worked to implement policy to regulate FRT



Ban Facial Recognition Interactive Map

Other Concerns and Bans Surrounding Facial Recognition Technology (FRT)

- New York's ban on FRT in schools follows an analysis revealing greater risks associated with its use than benefits. Originally implemented to prevent school shootings, its efficacy has been questioned due to higher false positive rates among marginalized groups such as people of color, non-binary and transgender individuals, women, older people, and children.
- Rite Aid's decision to ban FRT from stores stems from a significant number of false matches, resulting in embarrassment and inconvenience for thousands of customers. As a result, the company has imposed a 5-year ban on FRT and plans to implement safeguards to prevent similar incidents in the future.x

Resources

- Federal Law Enforcement Use of Facial Recognition Technology
- Facial Recognition & Law Enforcement – The Value Proposition
- Police surveillance and facial recognition: Why data privacy is imperative for communities of color | Brookings
- Inside New Orleans' struggle with facial-recognition policing - POLITICO
- Metropolitan Police's facial recognition technology 98% inaccurate, figures show | The Independent
- Facial Recognition Is Accurate, if You're a White Guy - The New York Times
- When facial recognition does not 'recognise': erroneous identifications and resulting liabilities | AI & SOCIETY
- Facial recognition systems in policing and racial disparities in arrests
- A performance comparison of eight commercially available automatic classifiers for facial affect recognition | PLOS ONE
- Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.
- Ban Facial Recognition Map
- New York bans facial recognition in schools after report finds risks outweigh potential benefits | AP News
- Rite Aid banned from use of facial recognition in stores after thousands of false matches - ABC News
- Facial recognition used after Sunglass Hut robbery led to man's wrongful jailing, says suit
- Eight Months Pregnant and Arrested After False Facial Recognition Match - The New York Times
- Miami Police Used Clearview AI Facial Recognition in Arrest of Homeless Man
- Face Recognition Technology Accuracy and Performance | Bipartisan Policy Center
- Rite Aid "covert surveillance program" falsely ID'd customers as shoplifters, FTC says - CBS News
- How did facial recognition technology send the wrong man to jail where he was brutally attacked?

FROM POLICE ACCOUNTABILITY COMMISSION SUBCOMMITTEE

APPROVED AS TO FORM AND LEGALITY

_____

CITY ATTORNEY'S OFFICE

DAVIS CITY COUNCIL

ORDINANCE NO. _____

-

ORDINANCE: (1) AMENDING TITLE TWO OF THE DAVIS MUNICIPAL CODE (TITLE TWO) TO PROHIBIT THE CITY FROM OBTAINING, RETAINING, REQUESTING, ACCESSING, OR USING: 1) ANY FACE RECOGNITION TECHNOLOGY; OR 2) ANY INFORMATION OBTAINED FROM FACE RECOGNITION TECHNOLOGY.

WHEREAS, the City Council finds that the City of Davis has a moral obligation to protect its residents from persecution; and

WHEREAS, surveillance technology may threaten the privacy of all of us, surveillance efforts have historically been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, gender identity, immigration status, or political perspective; and

WHEREAS, the propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits, and the technology will exacerbate racial injustice, gender inequity, and threaten our ability to live free of continuous government monitoring; and

WHEREAS, multiple studies have demonstrated that Facial Recognition Technology performs poorly for darker skinned people and women[1]; and gender non-conforming folks; and

WHEREAS, the number of proven false arrests due to being misidentified by Facial Recognition Technology[2] has continued to increase due to expanding use of Facial Recognition Technology,

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF DAVIS DOES ORDAIN AS FOLLOWS:

SECTION 1. Title 2 of the Davis Municipal Code is amended to add Chapter 2.68 **AN ORDINANCE PROHIBITING THE CITY FROM OBTAINING, RETAINING, REQUESTING,**

[1] http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf
[2] https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

ACCESSING, OR USING: 1) ANY FACE RECOGNITION TECHNOLOGY; OR 2) ANY INFORMATION OBTAINED FROM FACE RECOGNITION TECHNOLOGY, to read as follows:

2.68.010. TITLE.

This ordinance shall be known as the Prohibition on Facial Recognition Technology Ordinance.

2.68.020. PERIODIC REVIEW.

The Davis City Council, on the advice of the Police Accountability Commission and relevant staff, shall review the effectiveness and appropriateness of this ordinance every five years, beginning from its effective date.

2.68.030. DEFINITIONS.

“City” means any department, agency, bureau, and/or subordinate division of the City of Davis as provided by Chapter 1-2 of the Davis Municipal Code.

"Face Recognition Technology" means an automated or semi-automated process that: (A) assists in identifying or verifying an individual based on an individual's face; or (B) identifies or logs characteristics of an individual’s face, head, or body to infer emotion, associations, expressions, or the location of an individual.

“Personal Communication Device” means a cellular telephone, a personal digital assistant, a wireless capable tablet, or similar wireless two-way communications and/or portable Internet accessing device used by City Staff, that has not been modified beyond stock manufacturer capabilities, whether procured or subsidized by a City entity or personally owned, provided that any bundled Face Recognition Technology is only used for the sole purpose of user authentication in the regular course of conducting City business.

2.68.040. PROHIBITING THE CITY FROM OBTAINING, RETAINING, REQUESTING, ACCESSING, OR USING: 1) ANY FACE RECOGNITION TECHNOLOGY; OR 2) ANY INFORMATION OBTAINED FROM FACE RECOGNITION TECHNOLOGY.

It shall be unlawful for any City staff to obtain, retain, request, access, or use: 1) any Face Recognition Technology; or 2) any information obtained from Face Recognition Technology, except for Personal Communication Devices as defined by Section 2.68.030. City staff’s inadvertent or unintentional receipt, access to, or use of any information obtained from Face Recognition Technology shall not be a violation of this subsection, provided that:

(1) City staff does not request or solicit its receipt, access to, or use of such information; and
(2) City staff shall immediately destroy all copies of the information upon its discovery and shall not use the information for any purpose, unless retention or use of exculpatory evidence is required by law; and
(3) Upon discovery of such use, City staff shall log such receipt, access to, or use of any such information, and at the next earliest opportunity provide a written informational report to the City Council for discussion and possible action at a regularly scheduled meeting describing such

use(s). Such a report shall not include any personally identifiable information or other information the release of which is prohibited by law. In its report, City staff shall identify specific measures taken by the City to prevent the further transmission or use of any information inadvertently or unintentionally obtained through the use of Facial Recognition Technology.

2.23.050. ENFORCEMENT AND PENALTIES.

(1) Any violation of this Chapter constitutes an injury, and any person may institute proceedings for injunctive relief, declaratory relief, or writ of mandate in the Superior Court of the State of California to enforce this Chapter. An action instituted under this paragraph shall be brought against the respective city department, and the City of Davis.

(2) A court shall award costs and reasonable attorneys' fees to the plaintiff who is the prevailing party in an action brought under paragraph 1.

(3) Any person who has been subjected to Facial Recognition Technology in violation of this Chapter, or about whom information has been obtained, retained, accessed, shared, or used in violation of this Chapter may institute proceedings in the Superior Court of the State of California against the City of Davis and shall be entitled to recover actual damages (but not less than liquidated damages of one thousand dollars ($1,000.00) or one hundred dollars ($100.00) per day for each day of violation, whichever is greater).

(4) Violations of this Chapter by a city employee shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements and in accordance with any memorandums of understanding with employee bargaining units.

SECTION 3. Severability.

The provisions in this Ordinance are severable. If any part of provision of this Ordinance, or the application of this Ordinance to any person or circumstance, is held invalid, the remainder of this Ordinance, including the application of such part or provisions to other persons or circumstances, shall not be affected by such holding and shall continue to have force and effect.

SECTION 4. Construction.

The provisions of this Ordinance are to be construed broadly to effectuate the purposes of this Ordinance.

IN COUNCIL, DAVIS, CALIFORNIA,

PASSED BY THE FOLLOWING VOTE:

AYES -

NOES -

ABSENT -

ABSTENTION -

ATTEST: _____

[CLERK NAME]
City Clerk and Clerk of the Council
of the City of Davis, California

Date of Attestation: _____

Proposed Amendments to Proposed Ordinance Forbidding Use of Facial Recognition Technology by the Davis Police Department

John E.B. Myers
Commissioner, Police Accountability Commission

Please ponder the following ideas regarding Facial Recognition Technology (FRT):

1. The Davis Police Department (DPD) shall not purchase FRT without prior approval of the City Council.

2. In the context of an ongoing police investigation, DPD may submit a photograph of a possible suspect to another law enforcement agency, and ask the other agency to employ FRT to uncover evidence that may link the suspect to the crime under investigation by DPD. Any submission to another agency must be approved in advance by command level staff at DPD. If another agency employs FRT and FRT analysis reveals evidence deemed useful to further investigation of the suspect by DPD, FRT evidence can be used in the investigative process. FRT evidence *alone* is not sufficient to justify arresting a suspect, obtaining a search or arrest warrant, or stopping a person for a brief investigative stop, often called a Terry stop based on reasonable suspicion. In other words FRT evidence—in its current state of scientific validity/reliability, with FRT's proven inaccuracy rate regarding some members of society—is not sufficient to rise to the level of reasonable suspicion required for a Terry stop. FRT evidence can be combined with other evidence gathered independently of FRT to rise to the level of reasonable suspicion for a Terry stop, probable cause to arrest, and/or probable cause for a warrant.

There are basically three types of interactions between citizens and police: (a) Consensual encounters in which the citizen is free to leave. During such encounters, which occur thousands of times a day across America, police are free to ask questions, and the citizen is free to interact with the officer or leave without responding to questions. Consensual encounters raise no issues under the fourth amendment. (b) Terry stops or brief investigative encounters, in which the citizen is not free to leave. To detain a citizen, an officer must have reasonable suspicion that the person committed, is committing, or is about to commit a crime. (3) Arrest. All arrests require probable cause, which is a higher level of suspicion than reasonable suspicion.

Under the language I'm proposing for the FRT ordinance, FRT evidence alone would not rise to the level of reasonable suspicion. An officer could approach a citizen based on FRT evidence and ask questions, but the citizen would be free to leave.

3. DPD should be permitted to use FRT to assist in investigations of missing children and missing adults, including children and adults sexually trafficked.

4. DPD should be permitted to use FRT to assist in investigations of child pornography to help identify child victims of sexual abuse.

There may be other uses of FRT that we should discuss, but I want to share these ideas to keep the issue in the forefront of our thinking.

A Complete Ban on Facial Recognition Technology Would be Bad Policy

Reasonable minds differ on FRT. On balance, a ban on use of FRT by the DPD would be bad policy and would undermine public safety.

- Virginia Code Annotated § 15.2-1723.2: Virginia law allows use of FRT to (1) "help identify an individual when there is a reasonable suspicion the individual has committed a crime," (2) help identify crime victims, including victims of online sexual abuse, (3) help identify victims of human trafficking, (4) help identify missing persons and witnesses to crime, (5) help identify deceased persons, and for other purposes.

- Montana Code Annotated § 44-15-106: Montana law allows use of FRT to investigate serious crime.

- 20 of 42 federal law enforcement agencies use FRT.

- The NYPD uses FRT to investigate crime.

- The National Academy of Sciences wrote: "[T]he committee concluded that an outright ban on all FRT under any condition is not practically achievable, may not necessarily be desirable to all, and is in any event an implausible policy . . . ."

- FRT was used to identify a perpetrator of child sexual abuse that the perpetrator video recorded for distribution on the dark web.

- A criminal defense attorney used FRT to clear a defendant who was falsely accused of causing a fatal car accident.

- In my opinion, an argument that crime is not common in Davis, therefore our police don't need FRT, is naïve and dangerous. Davis is home to 60,000 people. The town of Uvalde, Texas has a population of 15,000. The town of Newton, Connecticut is home to 27,000. My guess is the parents of murdered children attending Sandy Hook Elementary and Robb Elementary thought their children were safe in small town America. The truth is horrible crime can happen anywhere. It FRT helps solve crime in big cities, it can help solve crime in small towns. I would not want to be the one to tell the parent of a murdered or abducted child, "We could have saved your child, but we are not allowed to use facial recognition technology."

This is not the time to ban FRT. It is the time to draft sensible legislation to put guardrails on the technology that will reduce the likelihood of misidentification, while authorizing FRT to solve crime and save lives.

May 3, 2024

VIA E-MAIL ONLY

City of Davis
Police Advisory Commission
23 Russell Boulevard
Davis, CA 95616
E-Mail: PAC@cityofdavis.org

Re: Facial Recognition Prohibition

Dear Chair Horton and Members of the PAC:

We are a coalition of civil rights organizations writing to express support for Chair Horton's proposed face surveillance prohibition ordinance. This is a technology that poses a threat to people of color and facilitates biased government surveillance of our communities. The use of this technology by government agencies poses a unique threat to public safety and the well-being of people in Davis, regardless of the system's accuracy. Davis should refuse to allow government agencies to acquire or use it for at least three reasons: first, due to flaws in face surveillance systems; second, because such systems are frequently built upon biased datasets; and finally, because face surveillance would supercharge invasive and discriminatory government surveillance.

The biased algorithms and processes that power face surveillance technology pose a threat to people of color. Multiple tests of this technology indicate it is less accurate for darker-skinned people. Peer-reviewed academic research by researchers at MIT has demonstrated that prominent

facial recognition technology products perform more poorly for people with darker skin and women.[1] In 2018, a test of Amazon's Rekognition facial surveillance product by the ACLU of Northern California falsely matched 28 members of Congress with arrest booking photos.[2] Of those false matches, 39 percent were people of color, even though people of color only constitute 19 percent of Congress. In practice, an erroneous face surveillance system could misinform and influence a decision about how to approach a person, including the decision of whether to use force. These kind of flaw systems should not be used to make decisions about Davis residents' lives.

The databases that underlie facial recognition systems are frequently biased as well. Facial recognition systems are commonly connected to databases of mugshot photos. These photos are then used as a reference point when the system searches for matches of individuals in the world. But because mugshot databases reflect historical over-policing of communities of color, facial recognition "matching" databases are disproportionately made up of people of color arrested in our communities. If such systems are connected to officer body cameras or surveillance cameras, these communities may be unfairly targeted simply because they appeared in another database.

Finally, face surveillance gives the government unprecedented reach into our lives and will fuel discriminatory government surveillance. People should be free to go about their daily lives without the government knowing whether they visit a bar or an abortion clinic, march at a political rally, or attend a religious service. Yet with the flip of a switch, Davis could add face surveillance to public CCTV cameras, sensor-equipped smart streetlights, or even officer-worn body cameras, creating a citywide surveillance network that could track and recognize residents as they move across town. Face surveillance technology makes it easy for the government to learn these and other details of private lives, all with little to no human effort. And like the surveillance systems that came before, the harms will fall hardest on people of color, religious minorities, and immigrants.

If Davis builds a face surveillance database, it might also invite requests from other governmental entities such as ICE, in effect entangling local agencies in the federal government's deportation machine. At a time when public protest is at an all-time high and the federal government is attacking immigrants and activists, Davis should refuse to build face surveillance systems that could easily be misused for dangerous, authoritarian surveillance.

Face surveillance will not make the Davis community safer and could lead to grave harm. It would subject residents and visitors to continuous monitoring and potentially violent contacts with law enforcement if it produces erroneous results. Regardless of accuracy, systems built on

[1] Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research 81: 1-15, 2018, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Natasha Singer, Amazon Is Pushing Facial Technology That a Study Says Could Be Biased, New York Times, Jan 24, 2019, https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html.

[2] Jacob Snow, Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots, ACLU Free Future Blog, July 26, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

face surveillance will amplify and exacerbate historical and existing bias that harms immigrants, religious minorities, activists, and people of color. An identification—whether accurate or not—could cost people their freedom or even lives. Davis should refuse to go down this road.

According to Fight for The Future, twenty-five (25) jurisdictions across the country have banned the use of face surveillance technology, including five (5) in California.[3]

Facial Recognition Technology is anti-democracy and anti-privacy

We have both a human right, and in California, a state right to privacy. The United States Supreme Court has consistently ruled for decades that we have the right to be anonymous in public. As a people, we have never consented to law enforcement tracking and tagging us like cattle, without at least a reasonable suspicion of wrongdoing. We have never been forced to, nor agreed to, carry a visible ID around with us as we move about our lives. We have consistently said we do not need to identify ourselves walking around, yet with this technology, it is the equivalent of forcing us to identify ourselves to others simply by participating in modern day life and walking outside our front door.

No young person exploring their sexuality will be comfortable exploring a gay bar for the first time. Muslims will be reluctant to attend their mosques. Inter-racial and same sex relationships, individuals seeking reproductive or gender affirming care in this post-*Dobbs* world, these actions first occurred in the "underground", requiring privacy, before they became accepted as normal and/or eventually decriminalized. In a world of perfect surveillance, these types of social changes will no longer be possible, because the status quo will become cemented.

Privacy is the underpinning of liberty. Those liberties will disappear if we let this genie out of the bottle. A March 2019 David Binder Research poll conducted for the ACLU revealed that over 82% of likely Statewide voters, and 79% of likely Bay Area voters, **oppose** the government using biometric information to monitor and track who we are, and where we go[4].

There are already thousands of public and private cameras in place, just waiting for facial recognition technology to be coupled with them. We don't have to accept as inevitable that technology will creep further into our lives. The health of our democracy depends on our ability to occasionally say no – that this technology, more so than others, is too radical for use in our community.

Face Surveillance Has Already Led to Proven False Arrests

To date, all but one of the victims of proven false arrests due to the use of face surveillance technology have been Black individuals.[5] Misidentification is not the only concern.

[3] https://www.banfacialrecognition.com/map/
[4] https://www.aclunc.org/docs/DBR_Polling_Data_On_Surveillance.pdf

[5] https://www.theguardian.com/technology/2024/jan/22/sunglass-hut-facial-recognition-wrongful-arrest-lawsuit

> "In September, the Government Accountability Office warned that federal law enforcement agencies have run thousands of AI-powered facial recognition searches without having appropriate training requirements in place for the officials running the searches, highlighting the potential for misuse.
>
> The Federal Trade Commission has increasingly put companies on notice that the rising use of facial recognition and artificial intelligence has created "new threats to privacy and civil rights. The use of face- or iris-scanning technologies to identify consumers in places such as stores, airports or sports arenas could lead to increases in identity theft and impersonation, the FTC warned in a 2023 statement. It could also "reveal sensitive personal information about them — for example, that they have accessed particular types of healthcare, attended religious services, or attended political or union meetings."[6]

By saying no to use of this technology, Davis will join the many other municipalities that are sending a strong message to the market to stop developing these technologies.

Sincerely,

American Civil Liberties Union – Northern California
Anti Police-Terror Project
Asian Americans Advancing Justice – Asian Law Caucus
California Immigrant Policy Center
Electronic Frontier Foundation
Fight For The Future
Immigrant Legal Resource Center
NorCal Resist
Secure Justice

[6] https://www.cbsnews.com/sacramento/news/texas-macys-sunglass-hut-facial-recognition-software-wrongful-arrest-sacramento-alibi/