ACLU
AMERICAN CIVIL LIBERTIES UNION
Wisconsin

207 East Buffalo Street, Suite 325
Milwaukee, WI 53202
(414) 272-4032
aclu-wi.org

June 17, 2025

Chair Bielinski, Vice-Chair Capriolo, and Honorable Members of the Milwaukee County Board Committee on Judiciary, Law Enforcement and General Services:

The American Civil Liberties Union of Wisconsin appreciates the opportunity to provide comments in support of File #25-427- A resolution requesting the development of a comprehensive policy framework for facial recognition technology that does not suppress Fire Amendment related activities, violate privacy, or otherwise adversely impact individuals' civil rights and liberties.

At this point in time, the proliferation and use of surveillance technology by the Milwaukee County Sheriff's Office or any law enforcement agency should give everyone pause. We are already seeing how surveillance technology is being weaponized in real time. Data gathered from facial recognition, automated license plate readers, artificial intelligence, and other surveillance tools are being used to target and detain individuals. The Department of Homeland Security is rapidly expanding its surveillance interface in local communities for immigration enforcement. Surveillance is being used to monitor and prosecute political protesters, people seeking reproductive healthcare, LGBTQ+ individuals, and doctors trying to provide care.

These are not projections – these are present-day realities carried out by bad actors within the federal government and local jurisdictions.

While local law enforcement agencies—including the Milwaukee County Sheriff's Office—may have good intentions, history reminds us how quickly larger systems can override those intentions. Data collected in Milwaukee County does not stay in Milwaukee County. Once it enters a federal pipeline, it can be accessed, shared, and used in ways we cannot predict—or stop.

The ACLU of Wisconsin deeply appreciates the sponsors of this resolution for their leadership on this issue and we welcome the opportunity to provide feedback regarding the development of a comprehensive policy framework relating to facial recognition and other surveillance technologies currently used and proposed in Milwaukee County.

At a bare minimum, we urge Milwaukee County to adopt a framework requiring transparency and meaningful opportunities for democratic participation by residents akin to Community Control Over Police Surveillance (CCOPS) legislation passed in twenty-six other jurisdictions across the country.[1] **Milwaukee County residents should not be surveilled in secret. We deserve to know how we are being surveilled with our own tax dollars.**

[1] https://www.aclu.org/community-control-over-police-surveillance; https://www.aclu-wi.org/ccops

Current MSCO Policy and the Dangers of Unregulated Surveillance Integration

The MCSO Policy Manual[2] contains at least two policies related to surveillance technology—**Policy 333 – Public Safety Video Surveillance System** regarding video surveillance cameras and automated license plate reader (ALPR) technology and **Policy 610 – Unmanned Aerial System (UAS) Procedure** regarding drones. Notably, Policy 333 contains the following section:

> 333.3.2 INTEGRATEION WITH OTHER TECHNOLOGY
> The Agency may elect to integrate its public safety video surveillance system with other technology to enhance available information. Systems such as gunshot detection, incident mapping, crime analysis, license plate recognition, facial recognition and other video-based analytical systems may be considered based upon availability and the nature of agency strategy.
>
> The Agency should evaluate the availability and propriety of networking or otherwise collaborating with appropriate private sector entities and should evaluate whether the use of certain camera systems, such as pan-tilt-zoom systems and video enhancement or other analytical technology, requires additional safeguards.

This is particularly concerning in light of federal and local law enforcement agencies across the country taking steps to integrate facial recognition with drones, body cameras, and integrated public and private camera networks.

Facial Recognition Automates Discrimination

FRT consistently shows racial and gender biases that persist despite improvements in algorithm training data. Even under optimal conditions, FRT systems are not designed to positive identification. Rather, at most the technology provides an "algorithmic best guess."[3] The data used to train facial recognition algorithms is overwhelmingly skewed toward white male faces. As a result, these systems perform best on white men—and worst on those who exist at the intersections of multiple marginalized identities: Black women, trans people, nonbinary individuals, the elderly, and children.

Joy Buolamwini and Timnit Gebru's landmark 2018 study, "Gender Shades," revealed that commercial facial recognition systems had an error rate of just 0.8% for lighter-skinned men, but up to 34.7% for darker-skinned women.[4] Widely reported National Institute for Standards & Technology (NIST) testing in 2019 found FRT algorithms were up to 100 times more likely to misidentify Asian and African American people than white men, and that women and younger individuals were also subject to disparately high misidentification rates.[5]

[2] https://county.milwaukee.gov/files/county/sherriffs-department/Documents/Milwaukee-County-Sheriffs-Office-Law-Enforcement-Policy-Manual-2025.pdf

[3] "Does A.I. Lead Police to Ignore Contradictory Evidence?," The New Yorker (Nov. 13, 2023), https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence/; see also Nat'l Acad. of Scis., Facial Recognition: Current Capabilities, Future Prospects, and Governance 48–49 (2024), https://www.nationalacademies.org/our-work/facial-recognition-current-capabilities-future-prospects-andgovernance.

[4] "Study finds gender and skin-type bias in commercial artificial-intelligence systems," MIT News (Feb. 11, 2018), https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

[5] Patrick Grother et al., U.S. Dep't of Com., Nat'l Inst. for Standards & Tech., Face Recognition Vendor Test Part 3: Demographic Effects 2–3, 8 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf;

While some reports indicate that demographic differentials in false match rates have lessened for some algorithms, testing by NIST and academic researchers indicates that the problem persists.[6]

Wrongful Arrests: Real Harm, Real People

The error rate of facial recognition systems is not just a technical problem—it's a civil rights crisis. Many people across the country have already suffered wrongful arrests and detentions due to faulty FRT matches:

- Nijeer Parks[7] in New Jersey, Robert Williams[8] in Detroit, and Michael Oliver[9] in Ferndale, Michigan–all Black men–were misidentified by FRT and wrongfully arrested.
- Porcha Woodruff,[10] a pregnant Black woman in Detroit, was wrongly arrested based on an FRT match.
- Randal Reid,[11] a Georgia man, was jailed for days due to a false facial recognition match for a crime in Louisiana—a state he had never visited.
- Steve Talley[12] was wrongfully arrested twice in Colorado because of flawed facial recognition technology.
- Kylese Perryman[13]–a Black man in Minneapolis–filed a lawsuit after being arrested due to a misidentification by FRT.

Police say a simple warning will prevent face recognition wrongful arrests. That's just not true. Even when police heed warnings to take additional investigative steps, they exacerbate the unreliability of face recognition results.[14]

See also Drew Harwell, Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubt on Their Expanding Use, Wash. Post (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federalstudy-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

[6] Patrick Grother, U.S. Dep't of Com., Nat'l Inst. for Standards & Tech., Facial Recognition Vendor Test (FRVT) Part 8: Summarizing Demographic Differentials 15 (July 2022), https://pages.nist.gov/frvt/reports/demographics/nistir_8429.pdf.

[7] "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match," New York Times (Jan. 6, 2021), https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[8] "Man wrongfully arrested by Detroit police with facial recognition tech settles lawsuit," Detroit Free Press (June 28, 2024), https://www.freep.com/story/news/local/michigan/detroit/2024/06/28/man-wrongfully-arrested-with-facial-recognition-tech-settles-lawsuit/74243839007/.

[9] "Wrongful arrest exposes racial bias in facial recognition technology," CBS News (Nov. 19, 2020), https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/.

[10] "Eight Months Pregnant and Arrested After False Facial Recognition Match," New York Times (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.

[11] "Lawsuit: Man claims he was improperly arrested because of misuse of facial recognition technology," ABC News, (Oct. 3, 2023), https://abcnews.go.com/US/lawsuit-man-claims-falsely-arrested-misuse-facial-recognition/story?id=103687845.

[12] "Man arrested for bank robbery files $10 million suit against Denver Police Department," Denver 7 (Sept. 15, 2016), https://www.denver7.com/news/local-news/man-arrested-for-bank-robbery-files-10-million-suit-against-denver-police-department.

[13] "In lawsuit, Minneapolis man says facial recognition tech led to his false arrest," MPR News (June 28, 2023), https://www.mprnews.org/story/2023/06/28/in-lawsuit-minneapolis-man-says-facial-recognition-tech-led-to-his-false-arrest.

[14] https://www.aclu.org/news/privacy-technology/police-say-a-simple-warning-will-prevent-face-recognition-wrongful-arrests-thats-just-not-true

Protest Surveillance and the Criminalization of Dissent

Facial recognition is a powerful tool for identifying and punishing dissent. This kind of surveillance chills participation in democracy, especially when used without a warrant or oversight.

- In 2015, Baltimore police used FRT[15] amid protests against the police killing of Freddie Gray to find individuals with outstanding warrants and arrested them directly from the crowd, in order to disrupt, punish, and discourage protesters
- During the 2020 BLM protests, FRT was used to identify protestors from video footage in numerous cities including Washington, D.C.,[16] New York City,[17] and Miami[18]
- In Milwaukee,[19] MSCO deployed drones to surveil protesters in 2021; MSCO Policy 333 permits drones to be integrated with facial recognition technology

Lack of Transparency in Law Enforcement Use of FRT

Law enforcement often omits material information about face recognition use from warrant applications. Police have a constitutional obligation to provide accurate information in arrest and search warrant applications so judges can independently determine whether there is probable cause. However, police routinely overstate the certainty of face recognition matches and withhold details about FRT searches that would let judges understand why those searches lack reliability and are not a proper basis for probable cause. In some cases, police completely conceal the fact of their reliance on facial recognition.

Inadequate disclosures continue post-arrest, where prosecutors routinely resist turning over adequate information about FRT use as part of their pre-trial disclosure obligations under *Brady*[20] and related doctrines. In an unknown number of cases, the government fails to even notify defendants of the fact that FRT was used in the investigation, much less details of that use.

The Need for a Comprehensive Policy Framework

In light of these profound concerns with the use of facial recognition and its integration with other surveillance tech technology, we urge the committee to adopt this proposal and provide meaningful and accessible opportunities for the public to have a voice in the development of this framework.

[15] "Maryland's Use of Facial Recognition Software Questioned by Researchers, Civil Liberties Advocates," The Baltimore Sun (Oct. 18, 2016), https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html.

[16] "Facial recognition used to identify Lafayette Square protester accused of assault," Washington Post (Nov. 2, 2020), https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html.

[17] "NYPD used facial recognition to track down Black Lives Matter activist," The Verge (Aug. 18, 2020), https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram.

[18] "Cops in Miami, NYC arrest protesters from facial recognition matches," Ars Technica (Aug. 19, 2020), https://arstechnica.com/tech-policy/2020/08/cops-in-miami-nyc-arrest-protesters-from-facial-recognition-matches/.

[19] "Drone log sheds light on Milwaukee Sheriff's eyes in the sky," Wisconsin Examiner (July 19, 2022), https://wisconsinexaminer.com/2022/07/19/drone-log-sheds-light-on-milwaukee-sheriffs-eyes-in-the-sky/.

[20] Jaylla Brown, "We Don't All Look the Same: Police Use of Facial Recognition and the *Brady* Rule," Federal 74 Communications Law Journal 331 (2022), http://www.fclj.org/wp-content/uploads/2022/06/74.3.1_Police-Use-of-Facial-Recognition-and-the-Brady-Rule_Proof.pdf.