Hello,

As a resident of Madison, Wisconsin I do not feel comfortable with MPD or any other local government entity using facial recognition to identify people, particularly in light of the way MPD criminalizes young people of color. I do not feel safe with this technology in the hands of people like you, or interim police chief wahl.
Thank you for your time and consideration,
Jeff Tischauser, PhD
Lecturer in Communication
School of Design and Communication
University of Wisconsin-Stevens Point

I just want to add that the testimony from the police chief is troubling. Is he denying that there is a problem with racially disparate misidentification? Has he said how many false arrests of Black people and how many false convictions of Black people would he find acceptable in order to get the advantages the vendors promise their product would deliver?
The chief suggests that he would write a policy to minimize racial bias in the use of facial recognition technology. If that's a realistic solution, why hasn't he written a policy to do something about the general ongoing racial disparities in MPD arrests?
---------- Forwarded message ---------
From: Steve Verburg <stverburg@gmail.com>
Date: Wed, Nov 18, 2020 at 5:21 PM
Subject: [please vote to recommend ban on face recognition technology
To: <PDPSRC@cityofmadison.com>

Members of the Madison Public Safety Review Committee:

I'm writing in support of "Creating Section 23.63 of the Madison General Ordinances establishing a Ban on the Use of Face Surveillance Technology."

This technology needs to be banned from use by city of Madison agencies and employees. The only change in the proposal I would suggest would be to delete the exceptions, which appear to be designed to allow the technology to be used to invade what little privacy we still have if the invasion of privacy is done by a third party and not at the request of the city, or the technology is used in "benign" situations such as phone login systems. Even use for logging into a phone is undesirable. First of all, there are other secure ways to log into devices. Secondly, using dangerous technology for so-called harmless purposes is just a marketing practice aimed at overcoming resistance to the technology. In this case, resistance in vitally important to the preservation of civil liberties and privacy.

The reasons for banning this technology are too numerous to list here. The reasons for allowing use of this technology are hypothetical and based on the usual fear tactics "public safety" agencies use to build and preserve their empires.

This is yet another test of your willingness to reduce racist disparities in Madison. This technology isn't race neutral. Even if it was, your Madison Police Department isn't race-neutral. It continues to over-police people of color. Any additional tools you provide to the Madison Police Department will worsen this problem when you should be recommending policies and practices the reduce racist disparities.

Please recommend that this proposal be enacted without exceptions. We don't need it. It will be used to harm the people of Madison. The time for taking actions like the enactment of this ordinance is long overdue.

Sincerely,

Steve Verburg
District 16, Madison, Wisconsin

Please leave off with the facial recognition systems. This article discusses studies proving how damaging these systems are for marginalized people and public well being in general:

https://static1.squarespace.com/static/5b8ab61f697a983fd6b04c38/t/5ca3ddcb15fcc0a59411ff30/1554243020037/HoffmannSeattleTimesFaceRecOpEd.pdf?fbclid=IwAR0VhQH1DwMmPEacQX5LYv_CTshkB7MktNvZA4nu1hNDrA2dUnssQcWuuDw

We can’t stand for this.
Thank you ,
Amanda

My name is Benji Ramirez, you have already heard from me tonight imploring you to side with American Civil Rights, to listen to the guidance of the ACLU's concerns and to listen to the will of your communities most vulnerable.

Since so many people have expressed concern about human trafficking, I decided to send some data about the racial disparities concerning who is actually being trafficked. Seeing as the data points that the most affected by human trafficking are BIPOC, and the technology that will allegedly come to save them doesn't even recognize them over half the time, why does it make sense to implement something that costs the average citizen their civil liberties for a farce?
Thank you, and I hope you can make a reasonable decision and not conform to traditional bodies of power.

Benji

Dear Commission members,

Due to a snafu on the city website, I am not certain my support for the item on your agenda this evening regarding a ban on face recognition tech was properly registered. I believe this measure is item 5 on your agenda.

I fully support this measure in its current form and do not want to see it weakened or made more ambiguous in any way, nor would I want to see it deferred.There are numerous ways the police can already conduct surveillance unthinkable even a decade ago, but this type of software is like adding rocket fuel to the fire. Frankly, I do not trust any agency, corporation or individual with its use, especially in the absence of a well-formulated body of law which would at least attempt to regulate it. I'm not sure such a body of law could be written and effectively enforced.

Other jurisdictions have enacted such bans, and federal legislation has also been introduced in both the House and the Senate. You would not be on the leading edge of the law by creating this addition to the City's General Ordinances. Please do so with all due haste.

Sincerely,
Margaret Bergamini
454 N Few St
Madison, WI 53703

Dear Public Safety Review Committee,

I am writing to ask that you support the proposal to ban the use of facial recognition technologies by city departments. In addition, I ask that you pass the proposal as written, without any adjustments, revisions, or amendments that would alter the intended intent, comprehensiveness, and impact of this proposal. Multiple cities have taken this step already, countless studies have found a consistent pattern of inaccurate results on faces of color, and many wealthy and influential corporations have acknowledged deep flaws in these technologies.

A top of the committee’s agenda states:
The continued use of this tool will most definitely deepens the racial disparities and injustices that further harm the black and brown people in our community.

Thank you,
Angela Jenkins

Good afternoon,

I am writing to you to ask that you SUPPORT Agenda Item #4 at tonight's meeting, as written, a full ban. Facial recognition technology is riddled with serious problems and should not be implemented. As stated by Anna Lauren Hoffmann, an assistant professor at the University of Washington Information

School puts it, "The dangers of facial recognition technology cannot be overstated." She points to the fact that when Amazon's "Rekognition" system was tested it "falsely matched more than two dozen members of the United States Congress with criminal mug shots, including a disproportionate number of members of the Congressional Black Caucus."

While members of the United States Congress have ample ability to hire professional attorneys should they be falsely accused by this technology to clear their names, the VAST majority of members of our community do not. Please support Agenda Item 4. Thank you for your time.

Trina Clemente
2601 Myrtle St
Madison, WI 53704

Dear Public Safety Review Committee,
I have learned that the agenda item numbers may have changed for this evening's meeting, and I am writing to ensure that my registration to support the proposed ban on the use of facial recognition technologies by city departments will be recorded and counted in the appropriate manner despite the fact that the agenda item I originally registered support for may no longer align with this topic. I may no longer be available to speak for the public comment period now, but I again ask that you pass the proposal as written, without any adjustments, revisions, or amendments that would alter the intended intent, power, comprehensiveness, and impact of this proposal.
Thank you,
Amy Owen
3129 Buena Vista Street
Madison, WI 53704

Hi,
I am emailing in support of banning the use of facial surveillance technology item #5 in the agenda today.

Thank you,
Netalee Sheinman
118 North St.
Madison, WI
53704

Good Evening,

Facial recognition technology is inherently biased against BIPOC and youth. For that reason alone it should never be utilized. However, facial recognition tech would also further the bias already existing in the currently (and historically) racist criminal justice system/prison industrial complex.

Given that 40 different (including Electronic Freedom Foundation, the Consumer Federation of America, the Freedom of the Press Foundation, Media Alliance, the National LGBTQ Task Force and Patient

Privacy Rights) well-established groups in the United States have already called for a moratorium on facial recognition technology, I could not see how the Madison City Council could justify approving implementing an ordinance permitting such widely criticized and flawed technology.

I urge you to pass the ordinance banning facial recognition technology in the City of Madison.

Thank you for your time,
Beth Welch
552 Troy Drive
Madison, WI 53704

Hello,

I'd just like to say that I fully support banning use of facial recognition surveillance by the city, and especially by MPD. This surveillance technology, pushed by large out-of-state corporations like Amazon, removes any ability for citizens to opt out of invasive data collection. It acts as a black box, a Robocop, which removes accountability for police when the technology makes mistakes, as it so often does, especially when attempting to distinguish people of color. The legal and regulatory framework for facial recognition surveillance is sparse at best, allowing for unnecessary and disproportionate surveillance of law-abiding citizens, and creating tenuous justifications for the incarceration of activists, which deters citizens from exercising their right to free speech. As mentioned, this method of surveillance frequently cannot distinguish people of color, leading to illegitimate arrests of innocent people from marginalized groups already facing undue repression from police, and sentenced based on automation bias, the belief that technology is infallible, if they are lucky enough to survive their arrest. How long until another Tony Robinson, until a young man is gunned down by police led to the incorrect address by inaccurate surveillance technology? Please vote to ban this dangerous surveillance technology from our city, and continue the great work of the Public Safety Review Committee under the leadership of Brenda Konkel.

-Jack

Mx. Jack K. Phillips
They/Them
Graduate Student, Biomedical Engineering
University of Wisconsin-Madison

Dear PSRC members,

I'm writing in support of the proposed ordinance to ban use of face surveillance by all city departments, including MPD. Please recommend passage of this proposed ordinance, without amendment. Facial recognition technology infringes on privacy, raising serious 4th amendment issues. It can chill 1st amendment rights. And it currently has a serious accuracy problem, especially for non-white people, creating equity issues.

To start with the accuracy problem…

Here's what a 2018 study by a British nonprofit found:

The overwhelming majority of the police's 'matches' using automated facial recognition to date have been inaccurate. On average, a staggering 95% of 'matches' wrongly identified innocent people… Police forces have stored photos of all people incorrectly matched by automated facial recognition systems, leading to the storage of biometric photos of thousands of innocent people.

The inaccuracy is greatest for non-white individuals, non-binary individuals, and children. The American Civil Liberties Union (ACLU) demonstrated the problems with Amazon's Rekognition facial recognition system when it tested the software on the 535 members of Congress. Amazon's system incorrectly matched twenty-eight congresspersons to criminal mugshots; eleven of these twenty-eight false matches misidentified representatives of color (including the late civil rights pioneer John Lewis).

This inaccuracy has led to arrests of innocent individuals. For example, a Black Detroit-area resident, Robert Williams:

Williams subsequently wrote an article for the Washington Post, entitled "I was wrongfully arrested because of facial recognition. Why are police allowed to use it?". He noted:

Federal studies have shown that facial-recognition systems misidentify Asian and black people up to 100 times more often than white people. Why is law enforcement even allowed to use such technology when it obviously doesn't work? I get angry when I hear companies, politicians and police talk about how this technology isn't dangerous or flawed. What's worse is that, before this happened to me, I actually believed them. I thought, what's so terrible if they're not invading our privacy and all they're doing is using this technology to narrow in on a group of suspects?

An article on an extensive facial recognition program set up by the San Diego Police Department notes:

San Diego's massive, 7-year experiment with facial recognition technology appears to be a flop. Since 2012, the city's law enforcement agencies have compiled over 65,000 face scans and tried to match them against a massive mugshot database. But it's almost completely unclear how effective the initiative was, with one spokesperson saying they're unaware of a single arrest or prosecution that stemmed from the program.

Moreover, as Matt Cagle of the ACLU notes:

Even if this tech were to one day work flawlessly, do we want to live in a society where the government knows who you are, where you're going, the expression on your face?... Consider also that the history of surveillance is one of it being turned against the most vulnerable communities….

Facial recognition fuels racist policing and facilitates life-altering harm. This is precisely why cities across America are banning it. The government shouldn't be allowed to use tech that makes us less safe and less free.

The ACLU states:

We've exposed law enforcement's quiet expansion of face surveillance into our communities. Our team has demonstrated how the technology's numerous flaws can lead to wrongful arrests, use of force, and grave harm. We've explained how even perfectly accurate face surveillance technology would remain a grave threat to civil rights, enabling the automatic and invasive tracking of our private lives and undermining First Amendment-protected activity.

Woodrow Hartzog (Professor of Law and Computer Science at Northeastern University School of Law and Khoury College of Computer Sciences) and Evan Selinger (Professor of Philosophy at Rochester Institute of Technology) note that obscurity is one of the most essential aspects of privacy. Obscurity is the notion that, when information is hard or unlikely to be found, it is relatively safe. This is something people rely on all the time, in their expectations of privacy, as they move through their lives. In "Facial Recognition Is the Perfect Tool for Oppression", Hartzog and Selinger note:

It’s easy to think people don’t have a strong privacy interest in faces because many of us routinely show them in public. Indeed, outside of areas where burkas are common, hiding our faces often prompts suspicion.

The thing is we actually do have a privacy interest in our faces, and this is because humans have historically developed the values and institutions associated with privacy protections during periods where it’s been difficult to identify most people we don’t know. Thanks to biological constraints, the human memory is limited; without technological augmentation, we can remember only so many faces. And thanks to population size and distribution, we’ll encounter only so many people over the course of our lifetimes. These limitations create obscurity zones, and because of them, people have had great success hiding in public.

Recent Supreme Court decisions about the 4th Amendment have shown that fighting for privacy protections in public spaces isn’t antiquated. Just this summer, in Carpenter v. United States, our highest court ruled by a 5–4 vote that the Constitution protects cellphone location data. In the majority opinion, Chief Justice John Roberts wrote, “A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, ‘what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.’”

Some may argue that law enforcement should still be allowed to use facial recognition in certain narrow circumstances (e.g. child victims). But once the technology is set up, its use will never remain confined to those circumstances. An even in narrow circumstances, the harms are likely to outweigh any benefits. As Lindsey Barret (Georgetown University Law Center) writes in “Ban Facial Recognition Technologies for Children – and Everyone Else”:

Young people are another group for whom facial recognition technologies are more likely to be inaccurate, and for whom the use of those technologies poses risks distinct to them on the basis of their physical characteristics. Children often have even less control over their privacy than adults do, and facial recognition surveillance frequently targets children out of misguided attempts to protect them. The chill to free expression that results from awareness of surveillance through facial recognition may also have a particularly significant impact on their emotional and intellectual development. The fact that facial recognition technologies perform less accurately for children’s faces puts them at risk when law enforcement or school security systems use the technology. Many of these harms are similarly applicable to and deeply concerning for adults, but may be even more severe for children due to their immaturity and the fact that childhood and adolescence are tremendously formative for both identity and opportunities later in life….

Clearview AI, which has been heavily criticized for its privacy violative services, has been quick to tout the use of its product in cases involving children, including investigations into child sexual exploitation. The horrendous nature of those crimes may seem to reduce the need for scruples when it comes to the harms of these technologies, when in fact the sensitivity of the circumstances makes their problems even more concerning. The false identification of a victim could be deeply traumatic, and the false identification of an ostensible perpetrator could lead to tremendously damaging consequences for the wrongly identified.

Anna Lauren Hoffmann (Assistant Professor in the University of Washington Information School) states some of the key problems well:

The dangers of facial recognition technology cannot be overstated. Prominent critics point to pernicious biases — especially against dark skin or young faces — that haven’t been adequately addressed. When tested, Amazon’s own “Rekognition” system falsely matched more than two dozen members of the United States Congress with criminal mug shots, including a disproportionate number of members of the Congressional Black Congress. Further work has shown how such systems confuse cultural markers of gender or sexuality (like makeup and hairstyles) with physiological ones, effectively “baking in” harmful stereotypes that limit their effectiveness across populations.

More importantly, facial recognition is not happening in a vacuum. It is plugging into existing surveillance structures that threaten millions of Americans daily, enabling the real-time monitoring of individuals by instantly linking faces up to the many information systems already available. One glance, and your face can be tied quickly to local law enforcement records, FBI files, DMV data, financial information, social media profiles, and more.

None of this is hypothetical. Many state and local police departments already have much of this access — they just need your face to supercharge it.

Worse, these structures are already marked by deep inequality. Surveilling Americans has always been a skewed affair, with certain groups bearing more of the burden than others — from persistent monitoring of religious minorities and communities of color to the invasive questioning heaped upon the poor to the systematic tracking of protesters exercising their rights to speech and assembly. Such inequality cannot be addressed by mere “tweaks” to the system. In fact, if facial recognition worked flawlessly, it would only make matters worse. It would simply “perfect” unfair and stifling patterns of targeting and abuse aimed at historically vulnerable populations.

Facial recognition is not a benign extension of existing surveillance practices — it’s rocket fuel. We should reject anything less than a moratorium. Passing watered-down and permissive versions of the bill now will only allow face recognition to penetrate deeper into our lives while unmaking any appetite we might have for regulation in the first place.

As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.

One of the best reviews of the problems with this technology is from The Project On Government Oversight (POGO), a nonpartisan watchdog, that has just issued a report called “Facing the Future of Surveillance”. It starkly outlines the dangers to liberty posed by this technology. I’ll close with a long excerpt from this report:

A. Privacy and Fourth Amendment Protections

1. Privacy as a Vital Constitutional Principle

Advances in digital technology have created unparalleled capabilities for collection, storage, cataloging, and use of sensitive data about individuals. Facial recognition surveillance is a prime example of this in every respect. By exploiting an ever-growing network of cameras, the government can apply facial recognition technology to video footage and photographs in a broad range of areas to identify individuals and collect data about their locations, activities, and interactions. Modern computers facilitate mass retention of this information, and allow for the creation of databases of hundreds of millions of photographs that can be used to create facial recognition profiles of the entire populace. Whereas just several years ago it was impossible for a police department of any size to comb through such vast databases and find matching faces in a timely manner, now facial recognition technology allows police officers to do so in seconds.

As a constitutional principle embodied in the Fourth Amendment’s protection from “unreasonable searches and seizures,” privacy is meant to do more than create legal walls that mirror physical ones, and is not limited to situations where we are inside our own houses or conducting conversations via phone or letter. Rather, privacy as a constitutional principle is meant to check a democratic government’s power over its citizens, chiefly by limiting the amount of information it knows about us. As Justice Sonia Sotomayor warned in her concurring opinion in United States v Jones, permitting unrestricted use of innovative digital technologies that are “available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may alter the relationship between citizen and government in a way that is inimical to democratic society.”

In last year's landmark Supreme Court decision Carpenter v. United States, the Supreme Court took on the novel risks surveillance in the digital age pose, fully embracing the right to privacy. In an opinion focused on cellphone tracking, the Court declared that "the [Fourth] Amendment seeks to secure the privacies of life against arbitrary power" (emphasis added), a framing that notably focuses not on certain places or types of conversation, but rather on protecting details of each person's life against an ever-watching government. Perhaps even more explicitly, the opinion of the Court in Carpenter stated that "a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance."

Because the constitutional principle of privacy means placing checks on government power, it follows that privacy extends to some activities that take place in public. When the Court in Carpenter highlighted that location records "hold for many Americans the privacies of life" (emphasis added), it was emphasizing that Fourth Amendment privacy protections do not focus narrowly on privately owned places, but rather on people themselves, wherever they may be.

The importance of limiting government access to the private lives of citizens is highest for sensitive information. But quantity of information can raise its own privacy issues. In Carpenter, the Court highlighted that "a cell phone—almost a feature of human anatomy—tracks nearly exactly the movements of its owner," and therefore presents heightened risks to privacy.50 While cell phones may have become an extension of our bodies, our faces require no such metaphor; unlike cellphones, our faces are never able to be turned off, left behind, or cast aside. If our faces can be subjected to the same type of continuous surveillance as cellphones, strong limits on surveillance technology will be necessary to properly rebalance power between the government and the people.

2. Cataloging Sensitive Activities

Facial recognition amplifies the concerns of upending privacy and unbalancing power between the government and its citizens in a unique and especially troubling way. The Supreme Court's key fear in both Jones and Carpenter was that in the course of tracking location, the government would unearth individuals' most sensitive activities. As Justice Sotomayor highlighted, this form of surveillance could catalog "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."

Whereas GPS and cellphone tracking inevitably record individuals' visits to these places, facial recognition surveillance could be directed at these types of locations. A camera could be placed outside a mental health facility, a lawyer's office, a substance abuse treatment center, or myriad other sensitive locations, and, with facial recognition, government officials could compile a list of every individual who appears there. These individuals could be identified, or "metadata profiles" could simply be built, by creating face prints of people who engage in specific activities (for instance, "Addiction Clinic Attendee #371," "Firearm Store Shopper #746," "Planned Parenthood Visitor #925"), and stored en masse to be cross-checked and used at a later time. Using facial recognition in such a manner could allow the government to harvest information from broad video surveillance with minimal human labor and reduce that visual data to a form that is much more easily archived for potential later use.

Such data could be used for an immense array of future government activities, ranging from profiling, to selective law enforcement investigations, to applications for background checks, to evaluations for civil service employment opportunities.

Equally important is the potentially chilling effect on political and other types of participation, such as religious and community activities. While it is difficult to measure the cause of inaction, research demonstrates that surveillance chills participation in basic activities. This is particularly true of surveillance directed at sensitive activities and groups vulnerable to persecution.54 If individuals believe that each camera on the street is cataloging every aspect of their daily lives, they may begin to alter their activities to hide from potential surveillance. That is something we must avoid, and we can do so through sensible reforms which demonstrate that checks against abuse are in place.

3. Unchecked Location Tracking

Facial recognition surveillance threatens to become as powerful a method of finding and tracking individuals as are cellphone and GPS tracking. While the Supreme Court has imposed a warrant requirement for these other forms of electronic location tracking, no such limit exists for facial recognition. In time, facial recognition could become a uniquely powerful location-tracking tool because there is no “middle man” for government-managed cameras that controls access to the data; the entire surveillance system is managed and all relevant information is obtained directly by law enforcement. This makes independent checks and proper transparency and accountability all the more important. Currently China is the only known nation that has sufficiently advanced facial recognition surveillance networks for location tracking. One key difference limiting the US government’s ability to do the same is the relatively lower number of cameras continuously recording the public. However, as use of body cameras, CCTV, and public-private partnerships continue to expand, the capacity to use facial recognition for location tracking will expand as well, especially if law enforcement is able to use the technology to circumvent the rules for electronic location tracking that the Supreme Court has created over the last decade. Rather than demonstrating probable cause and obtaining judicial authorization to gather cellphone location data, officers may simply turn to facial recognition to bypass this process. This would undo well-established investigative procedural requirements, and risk abuse by removing independent oversight. Thus it is critical that legal standards for use of electronic location tracking be preserved as new technologies provide the same capacity for monitoring location that cellphones do today.

…..

D. Freedom of Expression and Association

1. Facial Recognition Endangers Anonymity and Obscurity

The ability to freely participate in First Amendment-protected activities such as protests, political events, and religious ceremonies without disruption or discouragement is fundamental to American democratic society. Yet these activities could be subjected to facial recognition surveillance simply by placing government cameras nearby. And officers increasingly wear body cameras while on duty near protests, raising the question of whether body cameras’ promised benefit of preventing misconduct or the risks of recording such sensitive activities are overriding. The ability to rapidly identify every participant at such events raises the potential for disruption, and the ability to catalog all participants raises the specter of selective law enforcement action, or even overbroad prosecution.

A necessary aspect of freedom of expression and association is group anonymity. Over six decades ago, the Supreme Court held that “Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.” In that case, NAACP v. Alabama, the key action at issue was the government demanding NAACP’s Alabama membership list. In the digital age, no such direct action is necessary to remove the anonymity of an organization’s members. A single camera outside the entrance or exit to a group’s events combined with facial recognition could produce a membership list without consent or even notification. And because such identification can be done with practically no expenditure of human resources, it can be conducted on a mass scale.

2. Facial Recognition Endangers First Amendment Activities

Facial recognition could be a tool to disrupt First Amendment-protected activities. Unrestricted, facial recognition could allow law enforcement to scan crowds during large protests, political events, or religious ceremonies, and then arrest any individual with an active bench warrant. Ability to effortlessly identify any bench warrant for any petty offense could enable arbitrary action and abusive targeting, such as against selectively targeted individuals attending “events of interest,” such as protests, political events, and religious ceremonies.

This was already observed on a small scale with Geofeedia—a social media-monitoring company—which admitted that Baltimore police used the service during protests to “run social media photos through facial recognition technology” to find individuals with “outstanding warrants and arrest them directly from the crowd,” with the goal of targeting individuals who were protesting.

Given the number of bench warrants for petty offenses that some municipalities maintain, it is entirely possible that facial recognition could become an “arrest-at-will” authority used to disrupt such activities on a broad basis.

Facial recognition could be used to, without immediate interaction, catalog all participants at First Amendment protected activities such as protests, political events, and religious ceremonies. For instance, an FBI presentation on facial recognition highlighted its ability to identify participants at presidential campaign rallies.

Facial recognition databases could also be developed based on First Amendment activities, with participation in these activities then used for police investigations or in relation to civil service employment.

3. Facial Recognition Could Chill First Amendment Activities

Even if pernicious uses of facial recognition do not occur, the possibility—either from government policy or malicious individuals acting in absence of necessary checks and oversight—could create significant chilling effects. If individuals believe that going to a protest could lead to a CCTV tagging them for arrest based on a years-old traffic ticket, they may choose to stay home instead. If someone fears attendees at a Muslim student event are being cataloged via facial recognition the same way “Mosque crawlers” who were recruited to participate in and spy on Muslim community events tried to build such lists for the NYPD Muslim surveillance program, they may avoid engaging with their religious community.

Such fears of and capabilities for abuse must be put to rest. Requiring independent authorization for facial recognition will serve as a critical means of preventing improper use, and of assuring the public that this powerful surveillance tool is properly limited. Limiting facial recognition to serious crimes would also prevent abuse, and additionally stop facial recognition from being used to create arrest-at-will authority for the type of selectively targeted activity against protestors that Geofeedia described.

4. Facial Recognition Endangers Press Freedoms

A free and functional press cannot be subject to overbroad surveillance. Congress has long established special protection for journalists concerning the search and seizure of their documents. Forty states and the District of Columbia maintain shield laws that offer a degree of privilege to journalists to protect their sources. Nonetheless, at-risk sources such as whistleblowers often take extraordinary measures to ensure the secrecy of their interactions, including eschewing even the most secure forms of electronic communication in favor of in-person meetings to avoid potential electronic surveillance. Modern surveillance powers force journalists to take extra precautions, such as leaving cell phones and other electronic devices with built in GPS at home. But facial recognition can be used not just to catalog activities, but also interactions. If it becomes a tool to pinpoint how individuals interact and meet with journalists, it could present significant roadblocks for journalists seeking to speak to sources and whistleblowers while preserving anonymity.

Thus, I ask you to support the proposed ordinance.

Sincerely,
Dr. Gregory Gelembiuk

Hello all,

My name is Elena Haasl and I am a junior at UW-Madison and also the D.5 Dane County Board Supervisor (campus area). I first off would like to thank you for your time and appreciate the hard work you on this committee. I am writing today to urge you to support agenda items #1 and #5. The Police Budget Subcommittee is a crucial addition to the work of the PRSC and is essential to ensuring that funds are allocated to important and enriching city services, such as mental health initiatives and education, instead of being disproportionately allocated to policing our most vulnerable community members. Agenda item #5 Creating Section 23.63 of the Madison General Ordinances establishing a Ban on the Use of Face Surveillance Technology should be a no-brainer to support. I'm sure you are all well aware of how technology can work in a way that is biased, unfairly targeting BIPOC citizens as threats or criminals. Furthermore, face surveillance technology is a huge infringement on people's rights. It's clearly intrusive and the police do not need the technology to further impede on the personal lives of citizens.

Thank you for your time. I hope you all make the decision that falls on the right side of history and support agenda items #1 and #5.

Elena Haasl

Afternoon members of the Public Safety Review Committee :

Please find attached an electronic copy of the Security Industry Association's letter of concerns regarding the Boston City Council's Ordinance to Ban Facial Recognition, which would prohibit any city government official from utilizing facial recognition technology or any information obtained using the technology in certain circumstances. Please feel free to reach out to me or my colleague Jake Parker, who will be speaking at tonight's meeting, if you have any questions concerning the attached documents. We are happy to address any follow up questions you may have.

Have a great rest of your day.

Drake Jamali
Manager of Government Relations
Security Industry Association (SIA)
8405 Colesville Road, Suite 500
Silver Spring, MD 20910
djamali@securityindustry.org
(p) 301.804.4707
www.securityindustry.org

Dear members of the Public Safety Review Committee,

I am writing in support of proposed ordinance 62413, the ban on facial recognition technology (previously agenda item number 5 on your publicly posted agenda for today's meeting). The rise of facial recognition technology is very worrisome to me. I feel like this technology is being used and abused without much regard to ethics or justice. I think we really need to take a step away from using it so that we can stop the trend of it being abused and so that our community has time to really understand the implications of the technology.

Best,

Stevi Parmentier
Eken Park Resident
District 12

Dear Public Safety Review Committee, My name is Kailea, and I'm a resident of the Vilas Neighborhood where I'm represented by Alder Tag Evers. I am emailing to ask you to support item 4 on your agenda today, which will ban the use of facial surveillance technology by all city departments including the police. Please adopt this ordinance as it is written now. Here are some reasons to support the ordinance as is. 1. Here is a column by Anna Lauren Hoffmann, an assistant professor in the University of Washington Information School.

https://static1.squarespace.com/.../HoffmannSeattleTimesF...

Excerpt:

The dangers of facial recognition technology cannot be overstated. Prominent critics point to pernicious biases — especially against dark skin or young faces — that haven't been adequately addressed. When tested, Amazon's own "Rekognition" system falsely matched more than two dozen members of the United States Congress with criminal mugshots, including a disproportionate number of members of the Congressional Black Congress. Further work has shown how such systems confuse cultural markers of gender or sexuality (like makeup and hairstyles) with physiological ones, effectively "baking in" harmful stereotypes that limit their effectiveness across populations.

More importantly, facial recognition is not happening in a vacuum. It is plugging into existing surveillance structures that threaten millions of Americans daily, enabling the real-time monitoring of individuals by instantly linking faces up to the many information systems already available. One glance, and your face can be tied quickly to local law enforcement records, FBI files, DMV data, financial information, social media profiles, and more.

None of this is hypothetical. Many state and local police departments already have much of this access — they just need your face to supercharge it.

Worse, these structures are already marked by deep inequality. Surveilling Americans has always been a skewed affair, with certain groups bearing more of the burden than others — from persistent monitoring of religious minorities and communities of color to the invasive questioning heaped upon the poor to the systematic tracking of protesters exercising their rights to speech and assembly. Such inequality cannot be addressed by mere "tweaks" to the system. In fact, if facial recognition worked flawlessly, it would only make matters worse. It would simply "perfect" unfair and stifling patterns of targeting and abuse aimed at historically vulnerable populations.

Facial recognition is not a benign extension of existing surveillance practices — it's rocket fuel. We should reject anything less than a moratorium. Passing watered-down and permissive versions of the bill now will only allow face recognition to penetrate deeper into our lives while unmaking any appetite we might have for regulation in the first place.

As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.

2. 40 groups have called for a US moratorium on facial recognition technology. The groups include the Electronic Freedom Foundation, the Consumer Federation of America, the Freedom of the Press Foundation, Media Alliance, the National LGBTQ Task Force and Patient Privacy Rights.

Article: https://www.technologyreview.com/.../facial-recognition.../

Letter from the 40 groups: https://epic.org/.../face.../PCLOB-Letter-FRT-Suspension.pdf

3. Here is an article by Malkia Devich-Cyril, entitled "Defund Facial Recognition. I'm a second-generation Black activist, and I'm tired of being spied on by the police."

https://www.theatlantic.com/.../defund-facial.../613771/...

4. Article by Birgit Schippers (in the U.K.) “Facial recognition: ten reasons you should be worried about the technology”
https://theconversation.com/facial-recognition-ten...
Excerpt:
The right to privacy matters, even in public spaces. It protects the expression of our identity without uncalled-for intrusion from the state or from private companies. Facial recognition technology’s indiscriminate and large-scale recording, storing and analysing of our images undermines this right because it means we can no longer do anything in public without the state knowing about it. We find ourselves in an incredible moment to make structural changes that will reimagine public safety and crime prevention. Please support that reimagining tonight by establishing a Ban on the Use of Face Surveillance Technology. Thank you, Kailea

---

PSRC members,

For your Nov I8 meeting, I registered a few days ago in support of agenda item 4 to ban facial recognition technology. I see now that you have changed that item to #5.

Please record my registration of support for the BAN on facial recognition technology, whichever agenda item it ends up being tonight.

Thank you,

Lindsey Lund
2141 E Dayton St
Madison WI

Public Safety Review Committee,

I support the adoption of a full, uncompromised ban on facial surveillance technology. The use of facial surveillance technology is a step far too far in trading liberty for security. Its use oppresses law-abiding citizens and has been shown to disproportionately affect marginalized groups. It also is an incredibly imperfect technology that isn't fit even to accurately map people.

We are already too far down the path of too much surveillance and the path of freedom being completely exchanged for "security." We don't need to throw fuel onto the fire.

Support the ban on facial surveillance technology used by the state (agenda item #5) fully and without compromise.

Sincerely,
Andrea Parmentier
402 Pawling St, Apt 1
Madison, WI 53704

Dear Alders,

Please vote for the ban on facial recognition software. The harm caused by this technology far outweighs any benefits. If MPD didn’t engage so heavily in confirmation bias, this matter wouldn’t even be on the table.

This technology is especially harmful to BIPOC communities. It’s not a matter of opinion, it’s a fact.

Every vote against White Supremacy Racism matters. Every. Single. One. This one too. No excuses.

I’ve copied an exerpt from Dr Greg Gelembiuk’s letter. As per usual, he’s done his homework.

"1. Here is a column by Anna Lauren Hoffmann, an assistant professor in the University of Washington Information School.
https://static1.squarespace.com/.../HoffmannSeattleTimesF...
Excerpt:
The dangers of facial recognition technology cannot be overstated. Prominent critics point to pernicious biases — especially against dark skin or young faces — that haven’t been adequately addressed. When tested, Amazon’s own “Rekognition” system falsely matched more than two dozen members of the United States Congress with criminal mug shots, including a disproportionate number of members of the Congressional Black Congress. Further work has shown how such systems confuse cultural markers of gender or sexuality (like makeup and hairstyles) with physiological ones, effectively “baking in” harmful stereotypes that limit their effectiveness across populations.

More importantly, facial recognition is not happening in a vacuum. It is plugging into existing surveillance structures that threaten millions of Americans daily, enabling the real-time monitoring of individuals by instantly linking faces up to the many information systems already available. One glance, and your face can be tied quickly to local law enforcement records, FBI files, DMV data, financial information, social media profiles, and more.

None of this is hypothetical. Many state and local police departments already have much of this access — they just need your face to supercharge it.

Worse, these structures are already marked by deep inequality. Surveilling Americans has always been a skewed affair, with certain groups bearing more of the burden than others — from persistent monitoring of religious minorities and communities of color to the invasive questioning heaped upon the poor to the systematic tracking of protesters exercising their rights to speech and assembly. Such inequality cannot be addressed by mere “tweaks” to the system. In fact, if facial recognition worked flawlessly, it would only make matters worse. It would simply “perfect” unfair and stifling patterns of targeting and abuse aimed at historically vulnerable populations.

Facial recognition is not a benign extension of existing surveillance practices — it’s rocket fuel. We should reject anything less than a moratorium. Passing watered-down and permissive versions of the bill now will only allow face recognition to penetrate deeper into our lives while unmaking any appetite we might have for regulation in the first place.

As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.

2. 40 groups have called for a US moratorium on facial recognition technology. The groups include the Electronic Freedom Foundation, the Consumer Federation of America, the Freedom of the Press Foundation, Media Alliance, the National LGBTQ Task Force and Patient Privacy Rights.
Article: https://www.technologyreview.com/.../facial-recognition.../
Letter from the 40 groups: https://epic.org/.../face.../PCLOB-Letter-FRT-Suspension.pdf

3. Here is an article by Malkia Devich-Cyril, entitled "Defund Facial Recognition. I'm a second-generation Black activist, and I'm tired of being spied on by the police."
https://www.theatlantic.com/.../defund-facial.../613771/...

4. Article by Birgit Schippers (in the U.K.) "Facial recognition: ten reasons you should be worried about the technology"
https://theconversation.com/facial-recognition-ten...
Excerpt:
The right to privacy matters, even in public spaces. It protects the expression of our identity without uncalled-for intrusion from the state or from private companies. Facial recognition technology's indiscriminate and large-scale recording, storing and analysing of our images undermines this right because it means we can no longer do anything in public without the state knowing about it."

Sincerely,
Amelia Royko Maurer

Dear Members of the Public Safety Committee,

I am writing to ask that you fully support Item 4 on the agenda today as written, with no amendments. The ban on facial surveillance technology by all city departments including the police takes into account growing issues with this kind of technology, while still being flexible enough to allow the Madison PD to function and operate with its partners as before.

Portions of my PhD research focus on the use of technologies such as these by police departments across the country. As the Madison Police Chief has argued that such software is an especially helpful tool in certain child-search cases, we should first note the proposed amendment does not interfere with such a use case.

There are several concerns with facial surveillance, recognition, and other automated and predictive technologies used in law enforcement throughout the country however, and these justify a ban.

1) Racial bias – this is perhaps the most obvious and popular critique against such systems. As it stands now, facial surveillance and recognition technologies throughout the country continue to suffer from an inability to accurately identify non-white individuals as accurately as white individuals. This is a result of designer bias, incomplete and disparate data being used to 'train' these technologies, and has already had negative, tangible effects on people of color. This alone should be enough reason to adopt the proposed ordinance banning facial surveillance in the city as proposed, with no amendments.

2) Undue influence of private companies and 'lock-in' – less discussed, but equally important to consider is that technical solutions such as these are being provided by private companies which have no obligation to share their proprietary information. This means if a system was adopted and employed, it is highly unlikely that citizens – or even the PD – would have access to the internal elements of the system to try and understand how it works or to improve it if issues occur. Private companies with PDs across the country also enter them into non-disclosure agreements and other legal mechanisms to reduce what is even able to be discussed publicly about the technologies. This undercuts and is contrary

to the public deliberation essential to our own shared municipal governance. Further, once a technology is chosen, there is 'lock-in' where we tend to look for improvements from the same company due to its monopoly. This means alternatives and improvements in the future will be overlooked due to previous relationships (e.g. think about how you use Zoom without question now, even though alternative video platforms with the same functionality/less privacy concerns exist – you are 'locked-in' to the first choice made).

3) Investing in the community – much like the budgetary decision in weeks prior to not invest in further funding for the PD, a decision to ban facial surveillance is a moral action which demonstrates the city's commitment to its citizens. The proactive step of banning facial surveillance frees up the opportunity for investment into our community in more tangible ways, such as greater funds for our physical and mental health services, housing support, or neighborhood investment more broadly. Facial surveillance is being touted as the 'next generation of law enforcement' but we should recognize this for what it is: a private company advertising its services in the hopes of increasing sales. We should not purchase more unnecessary products and services; we should invest in our community instead.
Adopting the ban on facial surveillance in the city not only demonstrates a moral commitment to our city and citizens, it also counters a growing trend to employ technology with the hopes of 'revolutionizing' practices when really little changes. I am asking you to support agenda item 4 and ban facial surveillance in the city completely, with no amendments.
If you have any questions or would like any sources/data for the above points, please feel free to reach out to me.
Thank you,
Xerxes Minocher
10 Lakewood Gardens Lane, Madison, WI

Correction: Agenda #5

Begin forwarded message:
From: Gisela Wilson <giselawilson@gmail.com>
Date: November 18, 2020 at 11:09:41 AM CST
To: pdpsrc@cityofmadison.com
Subject: Supporting Item 4 on the Agenda (ban on use of facial surveillance technology)
PDPSRC@cityofmadison.com

17 November 2020

Dear Members of the Public Safety Review Committee,

I am writing in support of Madison adopting a ban on use of facial surveillance technology by all city departments, including the MPD (and, if possible, county law enforcement). I strongly support the ban and strongly oppose watering it down with amendments.

Many members of the public, including the MPD may argue against the ban on the basis of a "Nothing To Hide" argument —
an argument that has been soundly debunked for years (1). The obvious intrusions of data mining and potential for hacking various databases has only grown in the intervening time. Too many people fail to comprehend the vagaries of the methods of facial recognition technologies and will take the output as

fact, when it is no such thing. Facial recognition technology is NOT the problem-solver law enforcement will try to convince you of — it actually creates more problems than it solves. Law enforcement operates on timescale and with a false level of assurance in which correcting the repercussions for people's lives will be unlikely, if not impossible.

Facial recognition technology is NOT matching photos of similarly looking individuals and therefore is even more error prone (2). It is machine learning based on feature detection (such as eye spacing or the distance of the eyes from the mouth). Facial recognition technology is an extremely crude imitation of the early stages of neural processing used by our eyes and brain. Not even scientists who have spent their entire adult lives studying and researching visual processing understand how our brains draw the conclusion it does. Nor do the computer scientist have an understanding of the decisions made by machine learning and it is a practical impossibility to track down the logical (or illogical) path taken by machine learning.

Although facial recognition is only one part of the data puzzle, the use of facial recognition by law enforcement carries the most severe immediate repercussions — including unwarranted contact with law enforcement, illegal search and seizure and loss of civil rights. Facial surveillance is an unwarranted invasion of everyone's privacy with no probable cause. Since our privacy has slowly been eroded over the years, most people haven't really considered the various existential implications of privacy loss. The benefits to police are minor compared to the existential cost to everyone. "the problem with the nothing-to-hide argument is the underlying assumption that privacy is about hiding bad things"(1). "As a constitutional principle embodied in the Fourth Amendment's protection from "unreasonable searches and seizures," privacy is meant to do more than create legal walls that mirror physical ones, and is not limited to situations where we are inside our own houses(2)." As the Supreme Court has recognized, the concept of privacy needs to include a "privacy of life" that allows us freedom of association in public spaces and allows us to lose ourselves in the anonymity of a crowd (3).

Reasons Not to Trust the Nothing-To-Hide Argument —

A) Information Asymmetry and the Absence of Due Process increase the power imbalance between officials and individuals: Police (and the State) already have much more information about any specific individual than individuals have about them without adding facial recognition into the mix. Moreover, police are protected by qualified immunity, a powerful union, and the typically unquestioned authority our society has given the police. Facial recognition technology puts already vulnerable groups at even higher risk. Because it is a process involving illegal search and seizure, Facial Recognition technology is a violation of the Fourth Amendment.

B) Law enforcement and officials do not own databases and lack an understanding of database origins and vulnerabilities: Facial Recognition relies on databases the police do not own and the reliability and security of those databases will increasingly be vulnerable with time as data is passed through an increasing number of hands and data mining, data storage, and data marketing corporations. The problems increase exponentially as a function of hacking, alteration, and deep fakes. Photos can be tagged as "of interest", up-rated or down-rated not only by law enforcement, but also by the owners of the databases for a variety of reasons that have little to do with criminal activity (4)

C) Few people, including law enforcement understand the harms of data aggregation: Data aggregation "emerges from the fusion of small bits of seemingly innocuous data” (1). The entire data landscape is a distortion of data points (and photos) collected by businesses with self-interests other than an accurate representation of a individual, that person’s character and life.

D) Most people are excluded from knowing when data are collected and used against them. "people are prevented from having knowledge about how information about them is being used, and..they are barred from accessing and correcting errors in that data” (1). Even if aware of a mistake, due to the large number of data brokers, errors proliferate and it can be impossible for the average person to track down not only the source of an error, but all the databases it has been replicated into.

E) Secondary Use: Most databases used for facial recognition use photos obtained without an individual’s consent.

F) Nefarious actors: Once the databases exist, there is little to stop their use by stalkers and other nefarious actors, whether they are in law enforcement or not. In Brazil, people scrapping Facebook for revealing photos of children have created a market for pedophiles. Rather than allow for an expansion of its use, the more we can do to halt the market for facial recognition software the better.

H) Facial Recognition is error prone, with high false positive and false negative rates: It was only a few years ago that state-of-art facial recognition machine learning algorithms misidentified Queen Elizabeth as a shower cap and labelled people of color as apes. Recently, Amazon’s facial recognition technology recently mis-indentified over two dozen congressional representatives as criminals. Further, hairstyles, clothing, and make-up can cause mis-identification (5). The positioning of cameras, distance from the subject, differences in lighting, etc also affects measurements (2).

I) Nefarious actors — Once the databases exist, there is little to stop their use by stalkers and other nefarious actors, whether they are in law enforcement or not. In Brazil, people scrapping Facebook for revealing photos of children have created a market for pedophiles. Rather than allow for an expansion of its use, the more we can do to halt the market for facial recognition software the better.

J) Automation bias — People, including law enforcement, not understanding fallibility of databases and the algorithms used to search for a match will treat the output as fact.

(K) There is no clear legal or regulatory framework. Data mining is the wild wild West in the middle of a gold or oil rush. We are only beginning to understand its harms. Our laws and regulatory frameworks are decades behind.

(L) The existential threat mentioned at the beginning of this letter. "Privacy is not a horror movie, most privacy problems don't result in dead bodies, and demanding evidence of palpable harms will be difficult in many cases” (1). Without question, law enforcement is a context in which the palpable harms could result in a horror movie and dead bodies in real life. "Facial recognition is not a benign extension of existing surveillance practices— it’s rocket fuel. We should reject anything less than a moratorium”(5).

Forty groups have called for a moratorium on facial recognition technology (6). Various cities, including San Francisco and Somerville, Massachusetts have already banned it. Madison, if wanting to preserve democracy, free speech, privacy and individual civil rights should ban facial recognition technology, too.

Sincerely,

Gisela F. Wilson, PhD
1244 Morrison Ct
Madison, WI 53703

(1) Daniel J. Solove, "Why Privacy Matters Even if You Have 'Nothing to Hide'"
http://www.woldww.net/classes/Information_Ethics/Solove-ChronicleArticle-NothingToHide.pdf

(2) https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/

(3) Carpenter v. United States, 585 U.S. ____ (2018)

(4) Kashmir Hill, "The Secretive Company that Might End Privacy as We Know It"
https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

(5) Anna Lauren Hoffmann, "The privacy risks of uncheckedfacial-recognition technology"
https://static1.squarespace.com/static/5b8ab61f697a983fd6b04c38/t/5ca3ddcb15fcc0a59411ff30/1554243020037/HoffmannSeattleTimesFaceRecOpEd.pdf

(6) Angela Chen, "40 groups have called for a US moratorium on facial recognition technology" ,
https://www.technologyreview.com/2020/01/27/276067/facial-recognition-clearview-ai-epic-privacy-moratorium-surveillance/ ; Letter - https://epic.org/privacy/facerecognition/PCLOB-Letter-FRT-Suspension.pdf

(7) Beth Daley, "Facial recognition: ten reasons you should be worried about the technology"
https://theconversation.com/facial-recognition-ten-reasons-you-should-be-worried-about-the-technology-122137

To the Members of the Public Safety Review Committee:

I urge you to support the ordinance to ban use of facial surveillance technology by all city departments, including the police. There are ethical and moral concerns regarding this technology and its potential use. From The New York Times article, "Many Facial-Recognition Systems Are Biased, Says U.S. Study" December 19, 2019, "The majority of commercial facial-recognition systems exhibit bias, according to a study from a federal agency released on Thursday, underscoring questions about a technology increasingly used by police departments and federal agencies to identify suspected criminals. The systems falsely identified African-American and Asian faces 10 times to 100 times more than Caucasian faces, the National Institute of Standards and Technology reported on Thursday. Among a database of photos used by law enforcement agencies in the United States, the highest error rates came in identifying Native Americans, the study found. The technology also had more difficulty identifying women than men. And it falsely identified older adults up to 10 times more than middle-aged adults." Anna Lauren Hoffmann, Assistant Professor with The Information School at the University of Washington, writes in The Seattle Times article "The Privacy Risks of Unchecked Facial-Recognition

Technology", March 22, 2019, "The dangers of facial recognition technology cannot be overstated. Prominent critics point to pernicious biases — especially against dark skin or young faces — that haven't been adequately addressed. When tested, Amazon's own "Rekognition" system falsely matched more than two dozen members of the United States Congress with criminal mug shots, including a disproportionate number of members of the Congressional Black Congress. Further work has shown how such systems confuse cultural markers of gender or sexuality (like makeup and hairstyles) with physiological ones, effectively "baking in" harmful stereotypes that limit their effectiveness across populations."

40 groups have called for a US moratorium on facial recognition technology. The groups include the Electronic Freedom Foundation, the Consumer Federation of America, the Freedom of the Press Foundation, Media Alliance, the National LGBTQ Task Force and Patient Privacy Rights. Link to Article: https://www.technologyreview.com/.../facial-recognition.../
Link to Letter from the 40 groups: https://epic.org/.../face.../PCLOB-Letter-FRT-Suspension.pdf
Please join these groups and do what is ethically and morally right for our citizens, neighbors, friends, and family members and recommend to the Council that this ordinance be adopted as is, not amended (watered down).

Thank you for your time,
Lisa Hansen
1302 Dewberry DR
Madison, WI 53719

Good morning,

My name is Jennifer Summ, I live at 811 Silas St on Madison's east side.

I am emailing to support item four on the agenda for the Public Safety Review Committee meeting scheduled for 11/18/2020.

I support this ordinance and want it adopted as written. Not only is this technology dangerous and easily abused, but it is also full of holes and biases that continue to disproportionately affect communities of color and those in poverty. This is more likely to cause harm than to be helpful

Please adopt this ordinance as written and protect the people.

Kind regards,
Jen Summ

Dear members of the Public Safety Review Committee,

I am writing to support the full ban of facial recognition technology by all city of Madison departments, including the police department. Facial recognition technology is fraught with biases, and those biases are felt most keenly by our communities of color. It is unacceptable for our citizens to fear walking down the street and having their faces connected crime databases. Even if the software was 100% accurate, I don't think anyone reasonable would feel comfortable with the police being able to track them from place to place.

Please reject any amendments proposed to water-down this ban. Protect our citizens and our community by giving your support to the full ban and placing a moratorium on facial recognition.

Sincerely,
Erin Lemley
1703 Rowland Ave #1
Madison, WI 53704

Hello,

My name is Aryel Clarke and I am writing to indicate my support for the full ban on facial surveillance by all city of Madison departments. Facial recognition technology used in this way is a gross violation of privacy.

This technology is also built on data sets of primarily white middle-aged men, making them biased against anyone else, especially people of color. For example, a study cited by the ALCU found that Black women were misidentified by facial recognition technology 35% of the time (source). This illustrates how facial surveillance is not useful at best and racist and dangerous at worst. Misidentifications may lead to wrongful arrests, convictions, and increased police violence against innocent people.

Many other groups have spoken out against using facial recognition technology to surveil citizens, including Patient Privacy Rights, the LGBTQ Task Force, and the Freedom of the Press Foundation (source).

There is worry in the community that this proposed ban will not be enacted or be changed in a way that will greatly diminish its power to protect marginalized communities. I strongly urge you to adopt ordinance 4, the total ban of facial surveillance, as it is written.

Thank you,
Aryel Clarke
she/her/hers
UW Madison Dept. of Biomolecular Chemistry
Graduate Research Assistant

I am emailing to voice my support for ordinance 62413, which is agenda #4 at the upcoming PSRC meeting on November 18th.

Facial recognition software has many biases and other flaws, including that it has been shown to have substantial bias against people of color, falsely identifying African-American and Asian-American faces 10 to 100 times more often than Caucasian faces (https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html). Facial recognition is also one of the tools China is using to subjugate and commit human rights violations against Uighur Muslins (https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html), which is just one of many examples of how this technology can be misused. It is not at all a stretch of the imagination to be worried that the US would also misuse (or is misusing) this technology when you look at our history and unfortunately even our present. For these and other privacy / civil liberties reasons, 40 groups have called for a moratorium on law enforcement’s use of facial recognition software in the US (https://www.technologyreview.com/2020/01/27/276067/facial-recognition-clearview-ai-epic-privacy-moratorium-surveillance), citing in particular Clearview AI’s very concerning technology (https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html).

Facial recognition technology in law enforcement is not in the best interest of anyone in our society, especially not those who are already the most marginalized in our society. I encourage you to support agenda item #4.

Dear PSRC,

I am writing you to show my support for agenda item #4.
I want item #4 to be adopted as written, a full ban, not a watered-down ban.

1. Here is a column by Anna Lauren Hoffmann, an assistant professor in the University of Washington Information School.

https://static1.squarespace.com/.../HoffmannSeattleTimesF...

Excerpt:
The dangers of facial recognition technology cannot be overstated. Prominent critics point to pernicious biases — especially against dark skin or young faces — that haven't been adequately addressed. When tested, Amazon's own "Rekognition" system falsely matched more than two dozen members of the United States Congress with criminal mug shots, including a disproportionate number of members of the Congressional Black Congress. Further work has shown how such systems confuse cultural markers of gender or sexuality (like makeup and hairstyles) with physiological ones, effectively "baking in" harmful stereotypes that limit their effectiveness across populations.
More importantly, facial recognition is not happening in a vacuum. It is plugging into existing surveillance structures that threaten millions of Americans daily, enabling the real-time monitoring of individuals by instantly linking faces up to the many information systems already available. One glance, and your face can be tied quickly to local law enforcement records, FBI files, DMV data, financial information, social media profiles, and more.
None of this is hypothetical. Many state and local police departments already have much of this access — they just need your face to supercharge it.
Worse, these structures are already marked by deep inequality. Surveilling Americans has always been a skewed affair, with certain groups bearing more of the burden than others — from persistent monitoring of religious minorities and communities of color to the invasive questioning heaped upon the poor to the systematic tracking of protesters exercising their rights to speech and assembly. Such inequality cannot be addressed by mere "tweaks" to the system. In fact, if facial recognition worked flawlessly, it would only make matters worse. It would simply "perfect" unfair and stifling patterns of targeting and abuse aimed at historically vulnerable populations.
Facial recognition is not a benign extension of existing surveillance practices — it's rocket fuel. We should reject anything less than a moratorium. Passing watered-down and permissive versions of the bill now will only allow face recognition to penetrate deeper into our lives while unmaking any appetite we might have for regulation in the first place.
As a scholar of ethics and technology, the power facial recognition technology affords concerns me. As a mother raising a child against a backdrop of increased securitization and social instability, it terrifies and offends me.

2. 40 groups have called for a US moratorium on facial recognition technology. The groups include the Electronic Freedom Foundation, the Consumer Federation of America, the Freedom of the Press Foundation, Media Alliance, the National LGBTQ Task Force and Patient Privacy Rights.

Article: https://www.technologyreview.com/.../facial-recognition.../

Letter from the 40 groups: https://epic.org/.../face.../PCLOB-Letter-FRT-Suspension.pdf

3. Here is an article by Malkia Devich-Cyril, entitled “Defund Facial Recognition. I’m a second-generation Black activist, and I’m tired of being spied on by the police.”

https://www.theatlantic.com/.../defund-facial.../613771/...

Excerpt:
The right to privacy matters, even in public spaces. It protects the expression of our identity without uncalled-for intrusion from the state or from private companies. Facial recognition technology’s indiscriminate and large-scale recording, storing and analysing of our images undermines this right because it means we can no longer do anything in public without the state knowing about it.

Respectfully,

DJ Haugen
111 W Wilson St. #204
Madison, WI 53703
djhphoto@hotmail.com

I strongly support a full ban of facial surveillance technology, as written, no amendment.

If you're on the fence or do not support this ban, read on. Let's dig into the two main issues. One: the fourth amendment. Two: failures of AI and machine learning which uphold systemic racism.

First, facial recognition can be used without awareness OR consent. The U.S. Court of Appeals for the Ninth Circuit ruled that “the development of a face template using facial-recognition technology without consent (as alleged here) invades an individual’s private affairs and concrete interests.”

“In its recent Fourth Amendment jurisprudence, the Supreme Court has recognized that advances in technology can increase the potential for unreasonable intrusions into personal privacy…”

The courts have ruled that pervasive facial recognition is unreasonable and unconstitutional. Period.

Second, AI systems do not work how their vendors promise. They embed racism against vulnerable groups, which the vendors may not even be aware of until the systems are deployed. For more on that check the research of Timnit Gebru and others...

We don't need more AI to embed our systemic racism even deeper in our systems. We need less wrongful arrests, not more caused by faulty algorithms. How many false positive matches and wrongful arrests would you need, to see this technology as a bad idea? I would say the handful of problems we've already seen across the US are enough. Don't allow this tech into our city.

Bottom line: We should not enable our government, our police, our corporations, or ANYONE else to pervasively identify and track anyone (and everyone) as they go about their daily lives. And we should be even more worried that the systems never quite work as promised, and will further erode trust in policing.

Thanks,
Dan Fitch
Madison WI

Dear Public Safety Review Committee,
I am writing to ask that you support the proposal to ban the use of facial recognition technologies by city departments, and specifically that you pass the proposal as written, without any adjustments, revisions, or amendments that would alter the intended intent, power, comprehensiveness, and impact of this proposal. Multiple cities have taken this step already, countless studies have found a consistent pattern of inaccurate results on faces of color, and many wealthy and influential corporations have acknowledged deep flaws in these technologies. Our city urgently needs to avoid using tools with the likely result of widening racial disparities in law enforcement experiences and the justice system. Please pass this ban.
Thank you,
Amy Owen
3129 Buena Vista Street
Madison, WI 53704

Dear Committee Members,

My husband and I are asking each one of you to support Agenda item #4 to Ban Facial Recognition Technology. We support a Total Ban. As watchdogs for citizen safety in our city, it is important for you to safeguard the safety of all of our citizens. There is clear, available research to prove how this technology is not very accurate, especially with folks of black and brown skin coloring. This can - and has- lead to further discrimination and unjust practices towards people of color on top of the already racist system in play. Also, as a white couple, we don't want our faces on file for participating in activist events that are within our rights as good citizens, especially when the "powers that be" decide those activities challenge the white, dominant caste status quo and need to be quashed.

Thank you for supporting the (Total) Ban on Facial Recognition Technology.

Christine and Glen Reichelderfer
1042 Williamson St.
Madison, WI 53703

Dear Public Safety Review Committee Members,

Thanks for all you do in helping keep our city safe.

I am aware that you have a proposed ordinance coming up this week to ban the use of facial surveillance technology (agenda item number 4). Based on existing research, it's clear to me that this technology is not accurate and is particularly biased against people with dark skin. Also, the potential for misuse and certainly a decrease to privacy, even in public settings, is troubling to me.

Please vote in support of the ban. Thank you.

Julie

I ask for your support of item #4 a WRITTEN. Thank you.

Jill Annis

Public Safety Review Committee Members,

I am writing today to urge you to recommend the adoption of the proposed ban on the use of facial surveillance technology by any city employees, including MPD. Please recommend this proposed ban (agenda item #4) be adopted FULLY, as written by Alders Kemble, Evers, Martin, and Prestigiacomo.

Thank you,
Lee Alliet